S. HRG. 107–1151

NEED FOR INTERNET PRIVACY LEGISLATION

HEARING

BEFORE THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

JULY 11, 2001

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

88–997 PDF WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii	JOHN MCCAIN, Arizona
JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska
JOHN F. KERRY, Massachusetts	CONRAD BURNS, Montana
JOHN B. BREAUX, Louisiana	TRENT LOTT, Mississippi
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
RON WYDEN, Oregon	OLYMPIA J. SNOWE, Maine
MAX CLELAND, Georgia	SAM BROWNBACK, Kansas
BARBARA BOXER, California	GORDON SMITH, Oregon
JOHN EDWARDS, North Carolina	PETER FITZGERALD, Illinois
JEAN CARNAHAN, Missouri	JOHN ENSIGN, Nevada
BILL NELSON, Florida	GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Democratic Staff Director*
MOSES BOYD, *Democratic Chief Counsel*
MARK BUSE, *Republican Staff Director*
JEANNE BUMPUS, *Republican General Counsel*

C O N T E N T S

WITNESSES

NEED FOR INTERNET PRIVACY LEGISLATION

WEDNESDAY, JULY 11, 2001

U.S. SENATE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION
Washington, DC.

The Committee met at 9:30 a.m., in room SR–253, Russell Senate Office Building, Hon. Ernest F. Hollings, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. ERNEST F. HOLLINGS, U.S. SENATOR FROM SOUTH CAROLINA

The CHAIRMAN. We will commence the hearing with regard to Internet privacy, and I will file my statement. Let me summarize, because we need a sense of history.

The Congress has been front and center over the years with respect to protecting the people's privacy. We had the Federal Wiretap Act of 1968, the Credit Reporting Act of 1970, the Privacy Act of 1974; I authored the Cable Act of 1984 and heard some of the same misgivings by industry at the time. It has worked extremely well; the Video Privacy Protection Act of 1988; and of course, for what we are discussing for adults, we have got the Children's Online Privacy Act of 1998, all working extremely well. There is a question raised even again on Monday about the Financial Services Privacy Provisions, as to their effectiveness, in *USA Today*.

Otherwise, on the subject itself, the Federal Trade Commission has been toying with it for over 5 years. We have got listed here in our notes some nine hearings whereby they finally concluded after trying all the voluntary approaches, they recommended legislation. We now find a very interesting report that just came out from the Schwab Capital Markets on the Internet, and let me just quote this:

> "We disagree with corporate claims that a technology-neutral, selective opt-in mandate would likely make targeted marketing products prohibitively expensive to deploy or reduce the overall margins and profitability of advertisers. We also disagree that opt-in consent would have a substantial disruptive impact on the Internet in general. In our view, the experience of online opt-in consent business models suggests that the consumers can be enticed to provide personal and nonpersonal information at relatively little cost to web sites. We believe that the additional cost to entice people to opt in are likely to be overshadowed by the increase in revenues."

That is the best of the best business analysts. And, finally, of course, we are sort of behind the curve in the sense that the Europeans have moved forward with their safe harbor provision, and some would say, "Well, they haven't enforced it". It just got in in the last 2 years. We have got 12 of the 15 states now complying,

but more than anything else, those in the business thinks it is going to be enforced, so they have filed and met compliance: Microsoft, Intel, Hewlett-Packard. We can go right on down the list.

So while we are wondering whether it is wise to require of American entities such as Microsoft, it is already being required, complied with, and they are happy in Europe.

[The prepared statement of Senator Hollings follows:]

PREPARED STATEMENT OF HON. ERNEST F. HOLLINGS,
U.S. SENATOR FROM SOUTH CAROLINA

Well—to quote former President Reagan—here we go again. Today the Commerce Committee will hold its first hearing on Internet privacy. It is past time for action on this issue, and I intend to introduce and report legislation to the full Senate before the end of this session.

Last year, after five years of diligent study, the Federal Trade Commission recommended that Congress pass Internet privacy legislation that reflects the time-honored fair information practices of notice, consent, access, and security. This recommendation was particularly credible in light of the FTC's record of extensive analysis on this issue and its two prior recommendations to allow self-regulation a chance to work. Where did self-regulation get us? Nowhere. As *Business Week* stated last year, "self regulation is a sham."

According to former FTC chairman Robert Pitofsky, "some sites bury your rights in a long page of legal jargon so its hard to find them and hard to understand them once you find them. Self-regulation that creates opt-out rights that cannot be found or understood is not really an acceptable form of consumer protection." Look no further than your mailbox to see that this is the case.

Pursuant to the Gramm-Leach-Bliley financial privacy rules, Americans have been receiving literally billions of notices in the mail alerting them that they can opt-out of the sharing of their personal financial information by financial institutions with third parties. These notices make a mockery of the claim that notice and opt-out provides sufficient protection.

Let me quote from the cover letter accompanying one of these notices:

> "We recognize that privacy is a very sensitive and important matter . . . [and] adhere to strict standards of security, confidentiality, and privacy with regard to consumer information . . . if you are comfortable with [our] handling of information we collect, you do not need to take any action at this time."

That sounds pretty good, your information appears to be safe and private. But the attached notice informs you that the company:

> "Reserves the right to share all information we collect . . . [including with] financial service providers, mortgage-bankers-brokers, securities broker dealers, indirect loan originators, correspondent lenders, transaction processors, insurance agent/companies, . . . retailers, others, such as non-profit organizations."

Taken together, the cover letter and the attached notice are in direct conflict and are deceptive. Quite clearly, this is concrete evidence of why opt-out doesn't work. And, if it won't work when they mail you the notice, it certainly won't work on the Internet when the notice is buried behind a link at the bottom of a web page.

Clearly we need legislation that requires notice, affirmative consent, reasonable access, and reasonable security to protect individuals online. Such an approach would not represent, as industry contends, a dangerous and unprecedented regulation of the Internet, but rather, a logical extension of existing privacy laws to this new medium. Congress has enacted numerous statutes to protect the privacy of telephone customers, cable subscribers, video renters, and credit card customers. The Internet should be no different.

Poll after poll indicates that the public wants this level of protection. Advances in technology have provided information gatherers the tools to seamlessly compile and enhance highly detailed personal profiles and histories. Moreover, news reports regularly inform us of privacy breaches of sensitive information on the Internet.

Last week, we learned that Eli Lilly inadvertently disclosed a list of hundreds of customers suffering from depression, bulimia, and obsessive compulsive disorder. Eli Lilly's response? An apology, and a promise it won't happen again. A year ago, the *New York Times* reported that 19 of the top 21 health sites on the Internet had privacy policies but "failed to live up to promises not to share information with third parties."

Obviously, fears about privacy are preventing the Internet from reaching its full potential. Some studies indicate that as many as 20 percent of all Internet users give false information online to protect their privacy. But there is a solution—privacy protection. Enacting privacy legislation will enhance consumer confidence in the medium and boost e-commerce. Forrester Research estimates that as much as $12 billion in online sales are lost annually due to concerns over privacy. We can change that.

As for industry claims that opt-in kills the Internet, they are just whistling Dixie. For example, a recent Arthur Anderson survey reported that 74 percent of people will be happy to opt-in to share their personal marketing information, if they believe they will receive something in return.

Some forward thinking companies already know this. The New York Times, Microsoft, Intel, Hewlett Packard, Expedia, Alta Vista, and Earthlink all provide opt-in protection, reasonable access to personal information that has been collected, and reasonable security for that information. Moreover, I note that some of these companies, Microsoft, Intel, Hewlett Packard, and one of the largest data collection companies—Axciom—have all signed on to the EU Safeharbor, which requires notice, opt-in for sensitive information, access and security.

If they can do it, we can legislate it—by establishing Federal standards that codify these "best practices." and, if we couple that privacy protection with preemption, which I am always cautious about. Congress can foster business certainty and consumer confidence and allow the Internet to flourish.

I want to put to rest fears that somehow legislation will shackle the Internet. The experts know that is not true. John Chambers of Cisco systems predicts that by 2010, a quarter of the world's global commerce will be conducted on the Internet. And Forrester Research group predicts that over $180 billion in online sales will occur by 2004. No legislation could ever stop, stifle, or thwart this inevitable progress.

I look forward to working with my colleagues on this committee to craft legislation in this area. Last Congress, nearly a majority of the Committee cosponsored legislation in this area. This year lets finish the job.

The CHAIRMAN. Let me yield to my distinguished former chairman.

STATEMENT OF HON. JOHN MCCAIN,
U.S. SENATOR FROM ARIZONA

Senator MCCAIN. Thank you very much for reminding me, Mr. Chairman.

[Laughter.]

Senator MCCAIN. I want to thank you, Mr. Chairman, for holding this hearing. The advent of network computers and developments like broadband television and wireless location technology make it much easier for businesses to track and to trade information about consumers' transactions, whereabouts, and preferences. For all the benefits that consumers derive from the customized services that this flow of information provides, surveys continue to show that Americans are concerned and should be concerned about their online privacy.

Last year, Members of Congress responded to these concerns by introducing various bills to restrict online collection, use, and disclosure of personal information. Three of these bills were introduced by members of this very Committee and referred here. While the bills were similar, they all addressed the elements of the Fair Information Practices: notice; choice; access; and security. They also differed considerably in what they prescribed.

With respect to consumer choice, for example, the question of whether the law should provide the consumer with either an opt-out or opt-in default was and remains an issue. Opt-out allows consumers' personal information to be used unless otherwise indicated,

as opposed to opt-in, which prohibits the use of consumer information in the absence of affirmative consent.

The difference is significant, considering that the vast majority of consumers probably will not change a default setting so that while consumers have choice under either regime, one significantly reduces the availability of personal information while the other does not.

The bills also differed on whether or not companies should be required to give the consumer access to all of the information gathered about them. Senator Kerry and I thought it would be unwise to mandate this, because it would require that separate pieces of information about an individual be gathered for the sole purpose of allowing a consumer to review them, and this would create a profile that might not otherwise be created. Moreover, a requirement that would allow consumers to access freely all data collected about them could compromise security and provide unintended consequences.

We failed to resolve these differences last year. I hope we can this year, Mr. Chairman. Since then, there have been developments that will and should enter the debate over what kind of legislation is needed. Following the Committee's hearings on online privacy last session, the Internet economy has continued to deflate, forcing companies to rethink their business models, and perhaps change the ways in which they collect and trade personal information.

The demise of some dot-coms bodes both well and poorly for personal privacy. On the one hand, the spate of dot-com bankruptcies and subsequent sale of customers' personally identifiable information to pay creditors demonstrates that this data is a real asset and one that may not always be used in accordance with stated policies. On the other hand, with investment capital no longer available to keep companies with nonsensical or nonexistent business models afloat, companies that are going to survive will need to compete more robustly for customers, and customer-friendly privacy policies are a way to do this.

The global implications of our information practices are also becoming more evident. Within the past year, numerous countries with whose businesses we routinely share personally identifiable information with, have passed laws restricting the handling of information about their citizens.

In November of last year, the Department of Commerce began registering American companies for the safe harbor agreement that it had negotiated with the European Union. The agreement gives American companies that adhere to strict privacy practices a measure of protection against enforcement of the European Union's privacy directive for the company's handling in Europe or elsewhere of information about EU residents.

Closer to home, since the Committee's last hearing on online privacy, final regulations controlling the use and disclosure of sensitive personal information regarding people's health and finances have been adopted and gone into effect. Some have charged that the restrictions are inadequate, and others complain that they're too onerous. Reacting to the characterization of the debate about privacy legislation is one that pits businesses against consumers. Since last year, a number of businesses have commissioned or pub-

lished studies purporting to show very significant costs, both the businesses' and the consumers', of restricting information flows.

Developments in the online industry self-regulatory regime, spurred by threats of legislation and consumer concern, have also occurred since last year. Some companies have revised their information practices to provide better notice and choice to consumers. Third-party advertisers, like DoubleClick, who have in the past been perceived as the skunks in the privacy debate, say they have made it easier for consumers to stop these advertisers from tracking their movements online.

Companies have also developed a range of software tools that protect privacy by anonymizing or encrypting information. Later this year, Microsoft and, I am sure, other companies will offer software that can electronically read a web site's privacy policy and compare the policy to the user's preferences regarding the placement of cookies.

In sum, these developments in foreign and domestic law as well as industry self-regulatory practices, should be considered as we debate the desirability of legislation to regulate businesses handling personal information. I remain convinced, Mr. Chairman, that a Federal law is needed.

I applaud the Chairman for continuing and commencing this debate on this issue, and I look forward to hearing from our witnesses. I am sorry, Mr. Chairman, for the unusually long opening statement. This is a very, very important issue to all Americans, and I am very proud of your leadership and continued involvement in this issue. I thank you, Mr. Chairman.

The CHAIRMAN. I appreciate it, and we are looking forward to working together and trying to get us a consensus built out of the Committee.

Senator Inouye.

STATEMENT OF HON. DANIEL K. INOUYE,
U.S. SENATOR FROM HAWAII

Senator INOUYE. Thank you very much, Mr. Chairman. I wish to commend you for convening this hearing this morning on this very important topic of Internet privacy.

Last year, I had the great privilege of co-sponsoring a measure that was authored by our Chairman, Senator Hollings, that I believe provided an excellent template for protecting individuals online. This year, I hope we can report a similar bill out of the Committee.

With that, Mr. Chairman, I ask that my full statement be made part of the record.

The CHAIRMAN. It will be included.

[The prepared statement of Senator Inouye follows:]

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

I am pleased the Senate Commerce Committee is holding this hearing today on the important topic of Internet privacy. Last year, I cosponsored legislation authored by our Chairman, Senator Hollings, that provided an excellent template for protecting individuals online. This year, I hope we can report a similar bill out of Committee.

The Internet is too vast and complex to leave privacy protection to self-regulation. While many companies employ excellent practices, there are thousands upon thousands of web sites with inadequate privacy policies. Moreover, despite their best in-

tentions, every incentive lies with companies operating on the Internet to collect and profit from individuals' personal information.

If individuals are willing to consent to such practices if they believe they may receive something of value in return, that is one thing. But most companies choose instead to set forth confusing, and misleading privacy policies that only offer Internet users an opportunity to "opt-out" of the collection and sale of their personal information.

Often times these opt-out policies are hard to read, hard to understand, and hard to find. To me that is not adequate consumer protection. That is why I believe we need to set forth a strong Federal standard—that is consistent with past laws on protecting privacy, for example in the Cable Act. There, cable operators were required to get prior consent ("opt-in") from subscribers before sharing information about individual subscriber viewing habits. This sensible rule has been on the books for seventeen years and it seems logical as a framework for use on the Internet. The Cable Act also requires that cable operators give consumers a right to access information that has been collected about them, and a right to seek damages in the event the law has been violated.

The notion that such protections are somehow too regulatory is somewhat curious to me. We have always put a priority on protecting privacy. The Internet should be no different.

I commend the Chairman for holding this important hearing. I look forward to our efforts in this area, and to the testimony of the witnesses today. Thank you.

The CHAIRMAN. Senator Rockefeller.

Senator ROCKEFELLER. I have no statement.

The CHAIRMAN. Thank you.

Then Senator Wyden.

STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON

Senator WYDEN. Thank you, Mr. Chairman. I will be brief. I just wanted to make a couple of points. First, Mr. Chairman I very much look forward under your leadership and working with Senator McCain to producing a bipartisan bill. I think it is a doable proposition. Senator McCain touched on the fact that a variety of Committee members have legislation, but I think under your leadership, we can put together a bipartisan bill.

It seems to me there are three or four key elements of consensus that the Committee can work around. First of all, I think it is clear that nobody on this Committee wants an *Exxon Valdez* of privacy. I mean, we cannot afford a disaster that would do enormous damage in terms of e-commerce and the private sector.

Second, it seems to me that we all understand that people's expectations in this field are very high, particularly as it relates to their personal information, financial information and health information. I don't think they want to put businesses through bureaucratic water torture for what amounts to, you know, paperwork exercises, but for their financial and personal information, the expectations are very high.

The last point that I would make, Mr. Chairman, is that I think perhaps the key challenge involved in trying to put together a bipartisan bill here involves the private sector in this country, and the question is really: Do they want one standard to govern the privacy rules in this country, or do they want 50? This involves the Federal and state relationship, and it involves the question of whether the private sector is going to have the U.S. Congress come in and in some way preempt what the states and the various localities are doing.

My message to folks in the private sector is that if they want some measure of preemption, they have got to support a bill with meaningful privacy protection. There has got to be meaningful privacy protection in order to have one standard rather than 50, and I think Senator McCain made a key point there. You have got to have those four elements of the Federal Trade Commission report in order to get over the bar that indicates you are for meaningful privacy protection, and I look to forward to working with you and our colleagues in getting it done.

The CHAIRMAN. Thank you.

Senator Allen.

STATEMENT OF HON. GEORGE ALLEN,
U.S. SENATOR FROM VIRGINIA

Senator ALLEN. Thank you, Mr. Chairman, and thank you for holding this hearing. This is an issue of concern to myself and many others, and I do want to associate myself with the remarks of Senator McCain and Senator Wyden. There are a lot of very good ideas. I look forward to working with all members of this Committee.

Senator McCain made a very good point on how the private sector is addressing this in Microsoft's P3P. Senator Wyden points out certain things that as we go forward with this, Mr. Chairman, I believe that when you are talking about privacy, there may need to be different levels of security based upon whether this is privacy dealing with health or whether it is finance, whether it may be consumer information.

I do think that if we go into this, we need to make sure the regulations are reasonable, that they are not over-burdensome as far as the Internet. The question and the results will affect how we can have access to goods and services to access for information to the education of our children, and how we entertain our families.

I will be guided by, I think, two principles here. One is that I believe that we should empower individuals, consumers, to make sure that they have the information necessary to be able to make a decision or a choice as to whether or not they want to enter into a specific site or not, and second, I think we need to encourage to the greatest extent possible reliable, credible self-regulation.

Now, as far as the states are concerned, I am wondering very much the rights and prerogatives of the states. However, this is clearly interstate commerce, and I think to have a patchwork of liabilities and rules would make it very, very difficult for business to know what rules and what liabilities they will have, and I do think that we need to be guided by certain principles, and they be nationwide in that regard.

I also feel, Mr. Chairman, that we talk about privacy, but really this is an issue of security, and most people understand that interacting in a society, you are going to have share information, whether it is on the Internet, whether it is credit cards, whether it is writing checks, whether it is answering a telephone call, whether having a telephone in your home, having a car registered. There is information being shared.

People are concerned about what happens to that information when they voluntarily choose to reveal it, and I think that we

ought to make certain that the personal information that they share is secure and will not be misused or abused.

So, Mr. Chairman, I thank you for bringing this very contentious issue. I have been analyzing all the bills that have been introduced before I became a member of the U.S. Senate, and Senator McCain certainly had an outstanding bill, from my perspective, last year. Senator Wyden also had—with Senator Burns had outstanding bills, and maybe there is a way we can come up with a bipartisan approach that empowers individuals, makes sure they are informed, makes sure they have the knowledge, but also trusts the private sector to the best that they all can react to this need to come up with standards that are credible and reliable.

So thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Senator Boxer.

STATEMENT OF HON. BARBARA BOXER,
U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Mr. Chairman, I ask unanimous consent to place my statement in the record. I will briefly, briefly summarize.

The CHAIRMAN. It will be included.

Senator BOXER. First, let me also commend you for making this a top priority. Senator McCain did, and I think it is so necessary to clarify the nature of the problem we are trying to solve, the degree of harm that consumers are suffering or might suffer, and the appropriate response, the right response, to that harm.

As a Senator from California, needless to say my deepest hope is that we can, in fact, reach consensus. This would be a tremendous thing, and I am really hopeful, given the nature of the comments here today, that we can do that. You have a record of doing that, and I certainly stand ready to do that. We want to address the consumer concerns, and we also want to help the Internet grow. We don't want to stand in the way of that. This balance is crucial.

Last year, I did work with Senators McCain and Kerry on their bill. I thought it was a balanced bill, but I stand ready to see if there are ways we can make that bill better and compromise and work with you, as long as we keep that basic goal of that balance between protecting the consumer and protecting the growth of the Internet, which I think is so key.

Let me just make one last point. I know the issue of spamming is not part of this debate. We have other times to look at the spamming question. But really in many ways, the whole issue of spamming is a privacy issue. It is when you are hit with those messages, so I trust that that also will move up on the agenda as something very important.

And, again, I look forward to working with you, your staff, and across party lines to reach a consensus on this.

The CHAIRMAN. OK. Good.

[The prepared statement of Senator Boxer follows:]

PREPARED STATEMENT OF STATEMENT OF HON. BARBARA BOXER,
U.S. SENATOR FROM CALIFORNIA

Mr. Chairman, thank you for calling this hearing on the increasingly important issue of privacy on the Internet. It is my understanding that this is only the first of a series of hearings we will hold on this issue this year.

I commend you for making this issue a top priority. These hearings are necessary to help clarify the nature of the problem we are trying to solve, the degree of harm consumers are suffering or stand to suffer, and the appropriate response to that harm.

I believe that with your leadership, we will be able to work together on this committee to find a policy solution that will respond to consumer concerns regarding their privacy on the Internet: and simultaneously help the Internet grow in the process.

A number of us on this committee, including myself, have taken an interest in passing legislation to protect privacy on the Internet. Though we have some disagreement on how to achieve that goal, I believe this and other hearings will help us air those areas of disagreement and reach a consensus.

I look forward to this hearing and working with you and your staff on this issue.

The CHAIRMAN. Senator Carnahan.

STATEMENT OF HON. JEAN CARNAHAN, U.S. SENATOR FROM MISSOURI

Senator CARNAHAN. Thank you, Mr. Chairman. The issues before this Committee today illustrate the profound impact that the Internet is having on our lives. The Internet boom has changed the way we communicate with others and the way we receive information and the way in which we engage in commerce. This innovation, however, is still in the growth phase, and I do not think any of us can accurately predict how the Internet will continue to change and develop, or what its future applications might be.

As the Internet has grown, though, so too have the concerns about the protection of personal privacy online. Such concerns have led to a debate about whether we should address online privacy through legislation, and if so, how that legislation should be crafted. I think that a number of key factors ought to be considered when assessing the need and the scope of online privacy legislation.

Obviously understanding the nature of a user's concern will be of paramount importance. I have seen survey data suggesting that a majority of Internet users in the United States have at least occasionally altered their online behavior because of privacy concerns. It is difficult to discern, however, the precise nature of Internet users' privacy concerns.

Are people worried primarily about identity theft? The security of their credit card or other sensitive information? Or are people uneasy about the collection of personal information being used for marketing purposes? We will need to identify exactly what causes Americans to alter their online behavior in order to respond appropriately.

I am an active user of the Internet. I surf the web to get my news and to conduct research and to shop, and I even occasionally bid on an auction. It is extremely important to me to know exactly what information a web site is collecting about me and how they will use that information and to whom that information will be disseminated.

When considering legislation, we must also determine how our proposal will impact web sites and the companies who operate them. We must ensure that we don't do anything that would stifle

future growth and innovation of the Internet, and we must consider the impact that new technological advancements may have on the dynamics of the issue.

P3P, for example, has the potential to allow users to protect their own privacy by providing warnings about web sites that do not fit their privacy preferences. Innovations such as P3P may provide part of the solution to this problem. I believe that eventually a workable balance will have to be struck; a well-crafted legislative solution will set appropriate guidelines for web operators, one that will assuage users' concerns and ultimately lead to a more widespread use of the Internet.

And, finally, I think that Government should lead the way by example in terms of guaranteeing online privacy protections. The Office of Management and Budget under President Clinton issued privacy guidelines for all Federal agencies' web sites, but this should just be the start of the Government's efforts. I am working with state and local officials in my state in an effort to ensure that Missouri is on the leading edge of protecting the privacy of its citizens.

As we consider efforts to impose privacy guidelines on commercial web sites, I think it is imperative that Government demonstrate its commitment concurrently. Thank you, Mr. Chairman.

The CHAIRMAN. Senator, you will find out what is collected in the next campaign.

Senator CARNAHAN. I'm sorry?

The CHAIRMAN. I say, you will find out what they have collected in the next campaign.

Senator CARNAHAN. Oh, yes, sir.

The CHAIRMAN. You said you wondered what.

Senator Ensign.

Senator ENSIGN. No.

The CHAIRMAN. Thank you.

Senator Nelson.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Mr. Chairman, I just want to say what a pleasure it is to be a new member of this Committee. I am looking——

The CHAIRMAN. Delighted to have you.

Senator NELSON. I am looking forward very much to serving under your leadership and Senator McCain's leadership, and this is a great privilege for me.

The CHAIRMAN. Thank you very much.

Senator Rockefeller.

STATEMENT OF HON. JOHN D. ROCKEFELLER IV,
U.S. SENATOR FROM WEST VIRGINIA

Senator ROCKEFELLER. Mr. Chairman, I hadn't planned on speaking, but I wanted just to make two points. Number one, there has been this very interesting sort of cross-relationship of we want to protect privacy, but we don't want to do anything to prevent Internet growth, and it strikes me that when you are talking about jobs in the environment, you run into this kind of thing.

I mean, people always say, "Well, we can't protect jobs and environment," and that is often the case and sometimes it isn't. Sometimes it just isn't. Sometimes you have got to decide you are going to go this way or you are going to go that way. And it may be that this is one of those issues.

Some here have talked about—you know, I am very strongly for privacy, but we can't have any Internet regulation; we have got to let them do it themselves. I have to tell you that I have a very smart legislative assistant who just went through my recent computer stuff with Windows cookies, and, you know, I am highly offended by what I have in front of me, which is basically everything that I have looked at, not just including what I have looked at, but also the advertisements that came on while I was looking at something.

Now, it is all listed right here. This just a few days, and I don't like it, and it holds out to me the possibility of being watched. Now, I consider myself reasonably—I use that word carefully—reasonably sophisticated when it comes to the use and knowledge about technology. I work on these things hard as the Chairman knows. But I had no idea that I could get this. I knew that there were cookies around and there were other things around that could say where I was and what I was doing and, you know, it is sort of like using a cell phone. The advantage is nobody knows where you are calling from, and all of a sudden this comes up and says, "Well, they know exactly where you are calling from, what you are going to do, what you want".

And I consider this mildly dangerous. During the course of the questioning, I am going to be rather careful to ask people why they think that we passed nine pieces of privacy legislation. You mentioned a number of them, Mr. Chairman, aimed at everything from telephones, credit cards, to children over a number of years, and yet we allow this to go on, where virtually anything—my life, my disposition, my nature, my character, all of it is just sitting here for anybody to see and, in fact, print out. So this is going to be an interesting hearing.

The CHAIRMAN. And, in fact, sell.

Senator ROCKEFELLER. And sell.

The CHAIRMAN. That is right. Very good. I think that is all our colleagues, and we appreciate their attendance.

Mr. Marc Rotenberg, the Executive Director of Electronic Privacy Information Center; Fred Cate of Indiana University School of Law; and Dr. Paul Schwartz, professor of law at the Brooklyn Law School, please come forward.

The Committee has received these statements, and they will be included in the record in their entirety, but with the attendance here this morning and the other important panel that we have, we will ask that you try to summarize within 5 minutes or a little bit more as best you can, and like I say, the full statements will be included in the record.

Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you very much, Mr. Chairman. I would like to thank you and the other members of the Committee for holding this hearing today. I think over the last few years, there have been few Committees in Congress that have paid closer attention to the privacy issue than the Senate Commerce Committee, and I would like to thank you very much for your continued work on this matter.

There are very few issues today also in the United States where people seem to feel more strongly than on the matter of personal privacy. In poll after poll, the public has made clear that it is concerned about the loss of its privacy, and it believes that it is appropriate and necessary for the Government to act. This support is found across both political parties, across all demographic groups.

One poll finds that 86 percent of Internet users favor opt-in privacy policies. According to *Business Week,* three times as many Americans favor government action on the privacy front over industry self-regulation. And perhaps the most interesting poll is the one recently released by the Gallup organization, which found that not only 66 percent of Internet users believe that the Federal Government should act, but support for privacy legislation increased in proportion to the activity and experience of Internet users.

In other words, the more people used the Internet, the more they became dependent on the Internet for their business work, for their private communications, for the type of information sharing and exchange that has become increasingly common, the more they felt it was appropriate to pass privacy legislation. And in many ways, this is not surprising.

If you look at the tradition of the development of privacy law in the United States, you will see, in fact, that Congress has typically passed privacy legislation when new communication services and new commercial environments have been created. This was true in 1934 when privacy protection was established for telephone service. It was true in 1984 when privacy protection was established for cable service.

Legislation promotes public confidence and trust. It rewards good business practice. It helps create new market places and new economic opportunities where consumers are given the assurance that their personal information will not be misused.

I think the key question at this point, Mr. Chairman and members of the Committee, is how to pass good privacy legislation, how to get a bill done that will contain the key elements that will make privacy workable in the online environment. Now, in my statement, I have outlined what I believe to be those key elements. I also publish a book that contains U.S. privacy law, and I will briefly summarize what I think is necessary to make privacy legislation work.

I think the key point, first of all, is that organizations have to be open and accountable in the collection and use of personal information. This is more than just having a privacy policy. It is more than just telling people, This is what we will do with your personal information. Individuals need to have the ability to see that information, see how it is used and who it is shared with others.

That's the approach that was taken, for example, not only with credit reports, but interestingly also in the Cable Act of 1984, which says quite clearly that cable subscribers have the right to "access all personally identifiable information regarding the subscriber collected and maintained by a cable operator." That right of access is key to public confidence in understanding how the personal information that they provide to business will subsequently be used.

I think it is also important in a good privacy bill to have a private right of action. This is the approach that was taken not only in the Cable Act but in the Video Privacy Protection Act and the Telephone Consumer Protection Act. Virtually every privacy bill that has been done by the U.S. Congress gives individuals the opportunity to receive a small award—we are not talking about exorbitant fees here; we are talking about $500 or $2,000—when they are able to establish that their personal information was misused in violation of Federal law.

Now, on the critical issue of preemption—and I know this is a difficult issue, because, of course, it is quite attractive from the business side to say, "How can we be expected to comply with 50 different state standards"; that seems to us an unreasonable burden, and I think we are sensitive to that concern.

But I would like to make two points in response. First of all, the tradition in this area, what has been done in the past with Federal privacy legislation, is to create a baseline and to allow the states to legislate upwards if they wish. This has been done for two reasons: one, out of respect for our Federal form of government, which allows the states to protect the interests of their citizens if they so choose; also out of recognition that states may be able to experiment in different legislative approaches, come up with options that may not have been developed in Washington or maybe not even by some of the other states that turn out over time to be more effective.

Federal preemption would effectively prevent the states from innovating in the privacy area, and I think this would be a mistake. My other argument against Federal preemption concerns the practical problems that consumers face today in the online environment. It is true that in the absence of Federal preemption, some businesses may face 50 different state laws that they would have to comply with, but let's consider now what consumers today on the Internet face when they surf hundreds or possibly thousands of web sites in the course of a few weeks or a few months.

Every one of those web sites could have a different privacy policy, and every time a consumer goes from one web site to the next, that person would effectively have to evaluate the adequacy of that privacy protection. I think the goal in this area has to be to establish fair and effective privacy legislation. I think it will be good for consumers, good for businesses, and I thank you again for the opportunity to appear this morning.

The CHAIRMAN. Thank you very much.

[The prepared statement of Mr. Rotenberg follows:]

PREPARED STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center (EPIC) in Washington. I have taught the Law of Information Privacy at Georgetown University Law Center since 1990. I am the editor of two books on privacy and have participated in many of the public campaigns over the past decade to safeguard privacy rights in the United States.

I'd like to thank the Committee for holding this hearing today and also for the hearings that were held during the past Congress to address public concerns about privacy. This is an enormously important issue of interest to a great many Americans. Simply stated, there is a widespread concern that in order to enjoy the benefits of information technology we will be forced to sacrifice personal privacy. The central challenge is how best promote the benefits of new technology and to preserve right of privacy and personal autonomy.

I believe that there are two questions before the Committee today. The first is whether legislation is necessary to protect privacy on the Internet. The second, if you agree that legislation is appropriate, is what are the key elements of a good privacy measure. I will focus my remarks on these two issues.

1. THE NEED FOR PRIVACY LEGISLATION

a. Legal Tradition

Legal tradition in the United States clearly shows that laws will be established to safeguard the right of privacy when new electronic services are provided. This was true in 1934 when the Congress adopted provision 605 of the Communications Act to ensure the privacy of communications sent by telephone and in 1999 when Congress passed the Wireless Communications and Public Safety Act to safeguard the privacy of location data in advanced network services.

With virtually every new technology that involved the collection of personal consumer information—from Cable television and video rentals to electronic mail and automated medical information—Congress has passed laws to safeguard privacy. It has established clear responsibilities for companies that collect personal information and has created rights backed up with legal sanctions for individuals who disclose information in the course of a commercial transaction.

These laws have promoted best business practices, promoted public confidence, and limited the misuse of personal information in the new electronic environments. In other words, these laws have encouraged public adoption of new services to the benefit of both consumers and businesses.

Some have said that there should not be different rules for the online world and the offline world, but there are two answers to this point. First, online commerce simply is different. Cookies, web bugs, online profiling and Spyware are all uniquely associated with the architecture of the interactive digital environment. Publishers in the print and broadcast media simply do not have the ability to collect personally identifiable information without the actual consent or participation of their customers. A newspaper advertiser does not know who was reading an ad.

But today with the Internet, advertisers do have the ability to track individuals. Techniques are available to profile individual preferences, oftentimes without the knowledge or consent of the profiled person. It is because of the very specific capability of the online environment to collect and record personal information that legislation is appropriate. And it is consistent with the tradition of US privacy law that such legislation be adopted.

b. Technology and Legislation Work Together

Key to the adoption of privacy legislation is that lawmaking and technological innovation can work together. Groups, such as EPIC, that favor privacy legislation have also worked to encourage the development of technical standards that allow Internet users to safeguard their data and protect their identity. One of the most popular features on our web site is the Practical Privacy Tools page which allows Internet users to surf anonymously, delete cookies, encrypt private messages, erase files, and filter ads.

We recognize that there are a range of technical and legal approaches that will help safeguard privacy. But we also believe that in the absence of a statutory framework, a type of privacy survivalism could easily result. Without consumer trust in new services, each person will be forced to adopt elaborate defensive measures to protect privacy in the most routine commercial transaction. Such an outcome could not be beneficial for the long-term growth of electronic commerce.

c. Public Opinion

There are very few issues today in which Americans have expressed a clearer opinion than on the issue of privacy. In poll after poll, the public has made clear that it is concerned about the loss of personal privacy and that it believes it is appropriate and necessary for the government to act. Large majorities are found in both political parties.

According to the Pew Internet and American Life Project, 86% of Internet users favor opt-in privacy policies. According to *Business Week,* three times as many Americans believe the government should pass laws now to safeguard online privacy as those who believe self-regulation is sufficient. According to Forrester Research, 90% of Americans want the ability to control the collection and use of their data. The Pew survey also found that more than 90% of Internet users thought companies should be punished when they violate their own privacy policies.

In a recent Gallup Poll, 66% of email users said that the Federal government should pass laws to protect citizens' privacy online. Most remarkable is that the Gallup organization found that support for legislation increased as the level of experience increased. Frequent Internet users—those who spend 15 hours or more online each week—are more likely to favor the passage of new laws (75%) than are infrequent users (63%). This finding is contrary to some of the earlier industry-funded polls that attempted to suggest support for legislation would diminish as use of the Internet increased.

The message here is clear: experienced Internet users understand the limitations of technical solutions and industry self-regulation. They want legal control over their personal information.

d. Experience with Self-Regulation

The argument for legislation is also made clear by the failure of self-regulation to safeguard online privacy and promote public confidence in network services. Public concern about the loss of privacy has grown almost in direct proportion to the self-regulatory programs. In many respects, this is not surprising. These programs encourage the posting of privacy notices, which have come to be called privacy warning labels that provide little actual assurance of privacy protection. If you go to a website and read a privacy policy, you will see quickly that these policies simply state the many purposes to which the information collected will be used. Few privacy policies make any meaningful attempt to limit the use or disclosure of data obtained.

Technical problems are also arising with self-regulatory initiatives. How do you provide a privacy notice to a person who tries to access a web site from a cell phone, a commercial application that may become increasingly popular in the years ahead? One solution now under consideration is to create special symbols that could be viewed on the cell phone display. Another privacy scheme sets out a confusing array of privacy choices that will likely exclude many people from commercial web sites where privacy rules could otherwise provide uniform protection.

Problems with self-regulation can also be found in certain market segments where industry has been left free to design its own privacy policies rather than to rely on better established legal frameworks. For example, the Network Advertising Initiative proposal sanctioned by the FTC allows Internet advertisers to continue to profile Internet users, based on only the availability of an opt-out opportunity. This is contrary to the general approach in other areas which establish legal obligations for those who create profiles on known individuals. Even more surprising is that to exercise a right to opt-out of routine tracking, Internet users must maintain on their computers a cookie from the company that would otherwise track them!

e. Government Searches

Many who oppose legislation for online privacy say they want to keep government off the Internet. But one practical consequence of failing to pass privacy legislation is that without legislation there is no protection for personal information held by third parties from government searches. Government agents are free to go to Microsoft, Yahoo, Amazon, or any company in possession of personal data without a warrant and obtain the data on these companies' customers whether or not it is directly relevant to a particular investigation. This is contrary to the approach that has been established for other new electronic services as well as the treatment of sensitive information in the offline world. It also demonstrates the failure of self-regulation: there is no procedure and no method of accountability when data is disclosed to third parties through legal compulsion.

f. The International Dimension

The need for privacy legislation is demonstrated also by the demands of global commerce which now allows consumers around the world to buy and sell products online. This is a very promising development but also raises substantial concerns about the protection of the personal information that flows across the network. Many governments have taken steps to develop privacy laws to safeguard consumer interests.

Although the US has not yet adopted legislation that might be considered adequate for purposes of the European Union Data Directive, the Safe Harbor Arrangement does offer a possible intermediate step that will provide some assurance of privacy protection for European consumers doing business with US firms. Moreover, US firms have realized that in adopting these standards for their relations with customers in Europe, it is now sensible to provide similar protections for customers in the United States.

Privacy legislation will help carry forward this process by encouraging firms to adopt standards for privacy protection that will be recognized in countries around the world. Establishing these privacy rules for the online marketplace will be critical for the continued growth of global commerce.

g. Emerging Challenges

Much of the privacy work of this Committee has focused on issues associated with the Internet. But there are new challenges ahead. A report from the Center for Digital Democracy makes clear that the televisions in homes that allow us to look out on the world will increasingly be looking back at us. Cameras in public places raise new challenges for local communities. Even the tracking of rental cars by GPS has provoked public concern.

I do not think Congress today can anticipate all of the new privacy challenges that will arise. But the passage of legislation to protect online privacy will carry forward an important tradition, strengthen public confidence, and provide the basis for future legislative efforts.

2. THE NEED FOR GOOD INTERNET PRIVACY LEGISLATION

If the case is made for legislation to safeguard the rights of Internet users, then the next question is how best to draft the bill. Previous legislation enacted by Congress provides a blueprint for legislation in this area. These laws reflect a reasoned consideration of the key elements for privacy protection in a wide range of areas. They have also helped enforce best practices within industry segments, promote public confidence in new services, and minimize that risk that information will be used improperly.

a. Openness and Accountability

The first requirement of a good privacy law is that organizations are open about their data collection practices and accountable to those whose information they gather. This is not simple a matter of posting a notice or a privacy policy on a web site.

The most effective way to ensure openness and accountability is to give the individual the right to inspect the data collected, ensure its accuracy and understand it use. This principle goes back to the Privacy Act of 1974 which grants every citizen the right to access and correct records maintained by Federal agencies, 5 USC § 552a(d)(1–4), and to the Fair Credit Reporting Act of 1970 which gives consumers the right to access their credit reports maintained by credit reporting agencies. 15 USC § 1681g(a).

This approach has been carried forward in privacy legislation developed for new electronic services. The privacy provisions in the Cable Act of 1984, for example, establish the right for cable subscribers to "access all personally identifiable information regarding the subscriber collected and maintained by a cable operator." 47 USC § 551(d). The Children's Online Privacy Protection of 1999 allows parents to obtain records of information collected on their children and request that certain information be removed. 15 USC § 6502(b)(1)(B)(i),(ii).

The right to access information about oneself held by others in the context of a commercial relationship is one of the key elements of effective consumer privacy legislation.

b. Meaningful Consent

Privacy law makes clear that consent must be meaningful and that this often requires prior express consent. For example, the Video Privacy Protection Act states that disclosure of personally identifiable information, such as the title or description of tapes rented, requires "informed, written consent of the consumer given at the

time the time the disclosure is sought." 18 USC § 2710(b)(2)(B). The privacy provision in the Cable Act requires "prior written or electronic consent" before a cable operator may collect any personally identifiable information that is not necessary to provide the cable service or detect unauthorized interception of cable communications. 47 USC § 551.

One of the reasons that privacy advocates and experts favor the opt-in approach is that it follows the common sense understanding of consent. If you look up the dictionary definition for consent, you will likely see "permission," "approval," or "assent." All of these terms imply an overt act, not a failure to act. This is the approach typically followed in privacy statutes.

c. Private Right of Action

Privacy laws have also typically included a private right of action that has empowered individuals and made it possible to hold accountable those who misuse the personal information in their possession. In crafting the liability provisions in privacy statutes, Congress has wisely incorporated a liquidated damages provision that provides a specific dollar figure for violations of the law. This is necessary because it is often difficult to assign a specific economic value to privacy harm.

The Cable Act, for example, allows for a civil action and the recovery of actual damages not less than liquidated damages of $100 per for violation or $1,000, whichever is higher. 47 USC § 551(f). The Video Privacy Protection Act specifies liquidated damages of $2,500. 18 USC § 2710(c)(2). The Telephone Consumer Protection Act allows individuals who receive unsolicited telemarketing calls to recover actual monetary loss for such violation or up to $500 in damages. 47 USC § 227(c)(5).

These awards are hardly exorbitant. But they do help ensure that the rights established by Congress will be backed up with remedies. In the absence of a private right of action, there is a very real risk that there will be little incentive for companies to comply with privacy standards.

d. Federal Baseline

Privacy laws enacted by Congress have typically not preempted state privacy laws. This is partly out of respect for our Federal form of government that grants states authority to safeguard the rights of their citizens, and also out of recognition that states frequently innovate in areas of emerging privacy protection. The bill to address genetic privacy, for example, which has now received bipartisan support, came about in part through a process of trial and error in state legislatures. Similar experimentation in the best ways to address video surveillance is currently underway.

In the Cable Act, states and franchising authorities may take further steps to enact and enforce laws for the "protection of subscriber privacy." 47 USC § 551(g). The Video Privacy Protection Act will "preempt only the provisions of State or local law that requires disclosure" otherwise prohibited by the section. 18 USC § 2710(f). Even the Telephone Consumer Protection Act left the state Attorneys General free to bring actions under the Federal statute and made clear that nothing in that law would "prohibit an authorized state official from proceeding in State court on the basis of alleged violation of any general civil or criminal statute of such State." 47 USC § 227(f)(6).

e. Cable Act as Model

Mr. Chairman, almost twenty years ago you introduced legislation to safeguard the privacy rights of users of new interactive cable services. Similar legislation was introduced at that time by Senator Barry Goldwater and by Senator Howard Baker. There was no question at that time that in the interactive environment associated with cable television services in the early 1980s significant privacy issues would arise. Customers would bank online, cast votes online, and express their political opinions. Congress wisely established privacy rules to safeguard the collection and use of personal information in that emerging communications environment. The privacy provisions in the Cable Act, although filling only a few pages, provide just about the most extensive protection of privacy to be found in US law. 47 USC § 551. Under that law, every consumer in the United States who subscribes to a cable television service receives certain basic privacy rights.

Cable providers must provide written notice to subscribers of their privacy rights at the time they first subscribe to the cable service and, thereafter, at least once a year. These notices must specify the kind of information that may be collected, how it will be used, to whom and how often it may be disclosed, how long it will be stored, how a subscriber may access this information and the liability imposed by the Act on providers.

Subject to limited exceptions, the Act requires cable service providers to obtain the prior written or electronic consent of the cable subscriber before collecting or dis-

closing personally identifiable information. The Act grants cable subscribers the right to access the data collected about them and to correct any errors. It also provides for the destruction of personally identifiable information if that information is no longer necessary. There is a clear Fourth Amendment standard that limits the circumstances under which government may gain access to our private viewing records. Finally, the law sets out a private right of action including actual and punitive damages, attorney's fees and litigation costs for violations of any of its provisions. State and local cable privacy laws are not preempted by the Act.

The privacy provisions in the Cable Act of 1984 make clear that Congress can pass sensible, workable and effective legislation for new interactive environments. It has done so on a bipartisan basis and those provisions have stood the test of time.

f. Consequences of Weak Legislation

It is conceivable that Congress would adopt a weak "notice and choice" privacy law that provides few substantive rights, preempts state law, and lacks a method of meaningful enforcement. Such a measure would likely produce the backlash that has resulted from the weak privacy provisions in the Financial Services Modernization Act. The warning notices mandated by that law have simply raised public awareness of the widespread sharing of personal information and the difficulty in protecting privacy under the opt-out approach. This approach fails to establish actual safeguards for personal data when it is collected.

The better approach is the one favored by forward-looking businesses and the one traditionally followed in privacy law: those who wish to make use of personal information have the affirmative responsibility to obtain meaningful consent, rights to access personal information held by others should be established, and methods for meaningful oversight should be established.

CONCLUSION

Mr. Chairman, Members of the Committee, the time has come to make clear that the right of privacy does not end where the Internet begins. There is now the chance to establish law that will allow users to enjoy the benefits of innovation and to preserve cherished values. We have the opportunity to carry forward an American tradition that has marched side by side with the advancement of new technology. But we may not have this opportunity for long. In the absence of clear legal standards, we could easily drift into a world of privacy notices and warning labels, where every keystroke on your personal computer is quietly recorded in the database of another computer, then to be merged with data beyond your knowledge or control. In the absence of good privacy legislation, that future seems likely.

Thank you for the opportunity to appear before the Committee. I will be pleased to answer your questions.

The CHAIRMAN. Mr. Cate.

STATEMENT OF FRED H. CATE, PROFESSOR OF LAW, INDIANA UNIVERSITY SCHOOL OF LAW

Mr. CATE. Thank you, Mr. Chairman, members of the Committee. It is a privilege to appear, and I want to offer my appreciation for your holding this hearing.

Given the limited time, I will address just a single issue, and this issue is addressed in some greater detail in my prepared statement, and that is the method by which consumer choice is manifest and particularly the debate between opt-in and opt-out that has occupied this Committee in the past and is present in the bills that have been introduced to date.

The problem with the discussion of consumer control—and it is in many ways a little dark secret that not many of us want to talk about publicly—is that very few people read privacy notices. In fact, very few people read any of the notices we are presented with on the Internet. We click through them. We accept the terms without reading them. For a number of reasons, we do not encounter these notices, whether they are sent by email or mail or other methods of communication.

In fact, the Post Office tells us that more than half of mail sent in this country, unsolicited mail, is thrown away without ever being opened. So when you put a privacy notice in a letter and you mail it out in that form, half are going to be thrown away before they are even seen, without ever being seen by the consumer.

It is for this reason that we see very low opt-out rates in this country, but it is also for this reason that we see very low opt-in rates. The size of those rates, the fact that so few people respond, reflects, in fact, very little about what their choices are or how that choice is presented. It reflects instead the fact that few of us want to make those decisions, want to be bothered to make them, want to be interrupted when browsing on the Internet to make them, and in fact, very few people do make those decisions.

So the question for Congress, it would seem, is what to do about online privacy in an environment in which people are most likely to ignore and not act on the notices that will be required or that are being voluntarily provided.

Under opt-out, when a consumer fails to respond, the service can continue to be provided, the information can continue to be used, and the consumer has the option, if he or she wishes, if he or she is worried about privacy, to opt out either then or at any time in the future.

Under opt-in, if the consumer either does not see the notice or does not respond to it, then the service, if use of the information is a condition of the service, cannot be provided. The service is terminated at that point.

I found myself facing a good example of this this weekend as I was downloading software from the Internet, and I was presented not only with an intellectual property agreement, which I did not read; I just clicked on "Accept", but then for the first time in my experience, with a privacy agreement, which I was forced to page through. I had to check on each individual page that I had read it, and when I reached the end of it, I clicked on "I don't accept", at which point the installer closed, because my only choice at that point was to accept or not to receive the service.

If you want your own practical experience for what this is like, you might try setting your browser so that it will ask before it accepts cookies. Most of the people who have tried this—and this is often, I believe, testified to before this and other Committees—find that after being interrupted 10 or 12 times asking, "Will you accept a cookie?", they set the default to "Accept all cookies." That is opt-in in its clearest form, and it drives consumers to accept everything.

Interestingly, if you set your browser to say, "No, I will not accept cookies", you are then driven off of many sites which you might otherwise desire to use.

Now, this is dealing with opt-in and the situation in which information is first being provided. We also must consider the situation of subsequent use of information or use of that information by a third party. Under opt-in, a notice must be sent out, presumably by email or mail or telephone call. But, again, we know historically a majority of those notices will be ignored, and therefore, opt-in results in a *de facto* no-information use rule with a dramatic effect on innovation, on competition, on the ability to provide new serv-

ices because of the simple inability to even get the consumer to focus on the choice.

Moreover, this is where the real cost to consumers—and that is the only cost I am worried about today—that is where the real cost to consumers is felt, by those multiple contacts, by more email not less, by the increased price of services because of having to include the cost of reaching the consumer who is trying to hard not to be reached.

It is for this reason that opt-in, even though we think of it as a consent mechanism, often creates only the illusion of consent, not the reality, simply the appearance. We can all feel better that we know consumers are having a chance to opt in or not opt in, but in reality, consumers don't have that chance, because they must opt in to get the service, the information is necessary to provide the service, or because we miss the notice altogether. We simply never have the opportunity.

Now, the Chairman mentioned the situation in Europe earlier, and I believe that this, what I have just testified to, in fact, reflects what we see in Europe, which is very little, in fact, virtually no enforcement of the opt-in provisions, especially online. In fact, privacy scholar Amitai Etzioni has written—and I quote:

> "It seems that this EU directive is one of those laws that is enacted to keep one group, privacy advocates and their followers, happy, and as a rule is not enforced, so that commerce and life can continue."

A study this past January by Consumers International bears out this result. After studying the most popular web sites in the United States and Europe, the study found that although they collected information at nearly comparable rates, U.S. web sites provided better privacy protection despite having no legal obligation to do so than European sites. In fact, the authors of the study wrote—and, again, I quote: "U.S.-based sites tended to set the standard for decent privacy policies."

Finally, let me just note in closing opt-in poses significant First Amendment issues, precisely because of the burden that it places on speech, on communication. The Supreme Court has struck down many ordinances that would have required affirmative consent before receiving door-to-door solicitations, communist literature, even patently offensive cable programming. It seems highly unlikely that the Court would uphold the law requiring affirmative consent before permitting the collection and use of basic and true personal information. Thank you, Mr. Chairman.

[The prepared statement of Mr. Cate follows:]

PREPARED STATEMENT OF FRED H. CATE, PROFESSOR OF LAW,
INDIANA UNIVERSITY SCHOOL OF LAW

Mr. Chairman: My name is Fred Cate, and I am a professor of law and director of the Information Law and Commerce Institute at the Indiana University School of Law in Bloomington, and Global Information Policy Advisor to the law firm of Hunton & Williams. For the past 12 years, I have researched, written, and taught about information laws issues generally, and privacy law issues specifically. I directed the Electronic Information Privacy and Commerce Study for the Brook ings Institution, served as a member of the Federal Trade Commission's Advisory Committee on Online Access and Security, and currently am a visiting fellow, addressing privacy issues, at the American Enterprise Institute.

I appreciate the opportunity to testify today. I would like to take advantage of the presence of my distinguished colleagues on this panel and limit my testimony

to two points: the ways in which requiring consumer "consent" for information collection and use burdens consumers and creates costs, and the extent to which requiring opt-in exacerbates, rather than ameliorates, the harmful impact of many privacy laws.

THE TRANSFORMATION OF PRIVACY LAW

Historically, U.S. privacy law focused on two broad themes. The first and most visible was preventing intrusion by the *government*. This is the context of virtually all constitutional privacy rights, and it reflects the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance, and only the government collects and uses information free from market competition and consumer preferences.

The second theme reflected in U.S. privacy law throughout the last century was preventing uses of information that *harm* consumers. When privacy laws did address privates-sector behavior, they were designed to prevent specific, identified harms. So, for example, the common law privacy torts of intrusion, public disclosure, and false light privacy all require that the conduct complained of be "highly offensive to a reasonable person,"[1] and the information disclosed must either be false[2] or "unreasonably place[] the other in a false light before the public."[3] Similarly, the Fair Credit Reporting Act, one of earliest privacy laws applicable to the private-sector, focuses primarily on correcting inaccuracies and assuring that credit information is not used in ways likely to harm consumers.[4]

Increasingly, however, the dominant trend in recent and pending privacy legislation is to invest consumers with near absolute *control over information* in the marketplace—irrespective of whether the information is, or could be, used to cause harm. Public officials and privacy advocates argue that "we must assure consumers that they have full *control* over their personal information"[5] and that privacy is "an issue that will not go away until every single American has the right to *control* how their personal information is or isn't used."[6] The National Association of Attorneys General's December 2000 draft statement on Privacy Principles and Background sets forth as its core principle: "Put simply, consumers should have the right to know and *control* what data is being collected about them and how it is being used, whether it is offline or online."[7] And virtually all of the privacy bills pending before Congress reflect this goal: "To strengthen *control* by consumers" and "to provide greater individual *control*."[8]

This dramatic expansion from focusing on information privacy only in the contexts of *government* collection and *harmful* use, to regulating *all* personal information in the marketplace, poses many issues. Two of the most important involve the capacity and desire of most individuals to exercise control over information about them, and the impact of the legal means by which they seek to do so.

THE LIMITS OF CONTROL

The problem is that most consumers, in practice, don't want to exercise that control over the information we disclose and generate. We don't want to take the time to make those decisions, we often lack the knowledge or experience to understand the decisions we are being asked to make, we rarely want to be held responsible for the consequences of our decisions (especially since we seldom understand them), and, most significantly, we consider the interruption of being asked a nuisance and, as a result, we resent it. This is especially true on the Internet, where speed and convenience are most highly valued.

In practice, consumers ignore virtually all privacy notices and authorizations. The U.S. Post Office reports that 52 percent of unsolicited mail in this country is discarded without ever being read.[9] This is especially true online. Unsolicited e-mail, even when sent by a company with which the recipient has a relationship, is not opened at about the same rate, privacy policies are widely ignored, and pop-up screens with terms and conditions are simply clicked through without ever being read. The chief privacy officer of Excite@Home told a Federal Trade Commission workshop on profiling that the day after 60 Minutes featured his company in a segment on Internet privacy, only *100* out of *20 million* unique visitors accessed that company's privacy pages.[10]

All of the available data on consumers opting out or opting in reflects this. Extensive experience with company-specific and industry-wide opt-out lists, and the recent experience of financial services companies providing opt-out opportunities in compliance with the privacy provisions of the 1999 Gramm-Leach-Bliley Financial Services Modernization Act, demonstrate that less than 10 percent of the U.S. population ever opts out of a mailing list—often the figure is less than 3 percent.[11] Privacy advocates often point to these figures as evidence that opt-out doesn't work.

However, opt-in rates are virtually identical if not lower. In fact, two major U.S. companies recently tested the response rates to opt-in and opt-out, by sending e-mail messages describing the same use of personal information to statistically similar subsets of their respective customer bases. One e-mail said that the information would be used unless the customer opted out. The other said the information would not be used unless the customer opted in. *In both tests, the response rates were the same for both sets of messages: customers did not respond to either.*

THE OPT-OUT-OPT-IN COMPARISON

The question then for Congress, as you consider the need for any new online privacy legislation and the relative merits of opt-in and opt-out, is what is the impact of any new law on consumers, *especially in light of consumers' tendency to fail to respond to privacy notices of any form.* Both opt-in and opt-out give consumers the same legal control about how their information is used; under either system, it is the customer alone who makes the final and binding determination about data use. Therefore, the real focus of your inquiry must be on the burdens and costs imposed by each system.

While I and others have written and length about these issues in broad terms, I thought it would be most useful today to try to address these questions in the most specific manner possible.

Let's assume that Congress passes a law requiring that Web site operators provide a privacy notice and obtain some form of consent before collecting, using, or disclosing personal information. What would this mean in practice?

OPT-OUT

If *opt-out,* then the notice would be provided—much like 88 percent of commercial Web sites (100 percent of the busiest commercial Web sites) already do voluntarily and have done for more than a year[12]—in whatever form and including whatever terms Congress or Federal regulators required. The notice would include information about opt-out opportunities. That small percentage of the public who is acutely privately sensitive and today exercises opt-out opportunities whenever presented, would continue to do so and, importantly, would for the first time have the legal right to do so.

Most consumers, however, would continue to ignore both the notices and the opt-out opportunities, precisely as they do today. And, as a result of consumers not opting out, Web sites would be free to use information for any purpose that was within the scope of the privacy notice and that was not specifically prohibited by other laws. Consumers would get the same service, benefits, opportunities, and offers that depend on that information. *This is presumably what those consumers want, because if they did not, and if they felt sufficiently strongly about it, they could exercise their opt-out right at any time.*

Given the fast-changing nature of Internet services and technologies, it is unlikely that any privacy notice would cover all future uses of information. As new uses were developed, the Web site would be required to provide some form of prominent notice on the Web site or via e-mail (the precise details of how the notice must be provided would likely be set by Federal regulators). That notice would specify both a meaningful opportunity for consumers.to opt out and a sufficient amount of time for consumers to exercise their opt-out rights, before engaging in the new use. Again, it is reasonable to assume that most consumers would ignore the notice and the opt-out, but they would nevertheless receive whatever benefits or opportunities resulted from the use of their information. That is how online opt-out would work.

OPT-IN

If Congress' new law required *opt-in* consent for data collection, use, or transfer, the result would be quite different. Under opt-in, Web sites could no longer provide their privacy notices as they currently do or as they would under mandated opt-out, but instead would have to force every consumer to see the notice in an effort to obtain his or her consent to collect and use personal information. Presumably, the same small percentage of consumers who already read notices and worry about their privacy would continue to read privacy notices, but now they would have to do nothing to block use of their information. The substantial majority of other consumers who ignore privacy policies would also likely continue to do so.

Assuming the information was necessary to provide the service (for example, an address necessary to mail a book or airline ticket) or that the Web site chose to condition service on the consumer opting in, then the failure to opt in would mean no service. Both the minority of consumers who act on privacy policies, and the majority of the rest of us who simply ignore them, would be denied service. *Our privacy*

would be protected to be sure, but at the price of our not using the Internet. Consumers can obtain this type of privacy protection today—just by walking away from businesses whose privacy policies we disagree with—without the intervention of Congress.

For a sense for what this would be like in practice, set your browser to ask before accepting cookies. After you have been interrupted 10 or 12 times asking for consent to record information that is necessary to access the requested site, you will have a good feeling for what opt-in is like. If you click "No," you will be blocked from the Web page, so while you may have the satisfaction of being asked—again and again—you have no choice but to consent, unless you want to seek service elsewhere. *After having our Internet browsing repeatedly interrupted by opt-in requests to which we must accede to proceed, most Americans will be asking how to opt out of opt-in.*

As new uses for the information were developed, the operator would have to contact every consumer individually to ask him or her to opt in to the proposed use of the information. When most consumers failed to respond, presumably the Web site operator would try again and again to gain consent, thus increasingly burdening the consumer with more unsolicited e-mail, telephone calls, and/or mail, and increasing the cost of providing the new service or product for which consent was being sought.

We have some sense of what that cost and burden might amount to. U.S. West, one of the few U.S. companies to test an opt-in system, found that to obtain permission to use information about its customer's calling patterns (e.g., volume of calls, time and duration of calls, etc.) to market services to them required an average of 4.8 calls to each customer household.before the company reached an adult who even could grant consent, and cost almost $30 per customer contacted.[13] Some of those calls went unanswered, but others reached answering machines, children, and other household members and visitors who were ineligible to consent. Those individuals bore the burden resulting from the practical fact that it is much harder for businesses to contact consumers than for consumers to contact businesses—but this is precisely what opt-in requires.

A 2000 Ernst & Young study of financial institutions representing 30 percent of financial services industry revenues, found that financial services companies would send out *three to six times* more direct marketing material if they could not use shared personal information to target their mailings, at an additional cost of about $1 billion per year.[14] The study concluded that the total annual cost to consumers of opt-in's restriction on existing information flows—precisely because of the difficulty of reaching customers—was $17 billion for the companies studied, or $56 billion if extrapolated to include the customers of all financial institutions. And those figures do not include the costs resulting from restricting information-flows to reduce fraud, increase the availability and lower the cost of credit, provide co-branded credit cards and nationwide automated teller machine networks, develop future innovative services and products.[15]

The reason for this greater cost is easy to see. Under opt-out, a business wishing to use information about consumers can inform all potential consumers at once—through policies posted on Web sites, disclosures mailed to customer addresses, and other efficient, cost-effective forms of communications. The business doesn't even have to know specifically with whom it is attempting to communicate.

Consumers who object to a proposed use of personal information can prevent it by contacting the business via a toll-free telephone number, Web site, or pre-addressed response card. The communication can take place at virtually anytime—and therefore at the consumer's convenience—and the response mechanism can serve other business purposes. For example, the 800-number can reach a customer service center that is staffed to answer a variety of customer questions and provide access to customer account information. The Web site can provide a wide range of information and services, in addition to the opportunity to opt-out.

The comparative ease of communicating the privacy notice to the consumer, the flexibility of the customer being able to opt-out at his or her convenience, and the ability to spread the cost of handling "opt-outs" using systems that serve other functions does not mean that opt-out is without cost, but it does help to reduce those costs—both to consumers and businesses—significantly.

Moreover, the burden on consumers is multiplied by the fact that all of these contacts are just to obtain permission to examine data about customers to determine their eligibiliiy for a product or service offering. For those individuals who are eligible, a *second* round of contacts is necessary to actually make them to offer. It is difficult to imagine that this opt-in system will be perceived by consumers as anything more than an annoyance. U.S. West's customers displayed their annoyance at the intrusiveness required by opt-in. Only 28 percent opted-in when they were inter-

rupted with a call seeking consent, but 72 percent opted-in when the opportunity to consent was presented to the customer at the conclusion of a call that the *customer* initiated.[16]

Of course, this annoyance will be even greater for those people who do *not* qualify for the offer. For example, in the case of U.S. West, the telephone company was asking existing customers for permission to examine information about their calling patterns to determine their eligibility for new service plans and discounts. However, not all customers who consented actually qualified for the new service or discount. The burden and cost of contacting those customers who did *not* qualify were wholly wasted.

Under opt-in, the Web site operator has to contact all customers seeking their individual consent to examine data about them, even though many or most may not qualify for the offer. Because opt-in prevents businesses from using personal information to target their consent requests, it not only results in extra contacts with the consumers, but also exacerbates the burden of those contacts because they cannot be tailored to reflect consumer interests.

These same issues are presented by efforts to attract *new* customers by using personal information (such as their e-mail address) to contact them. Today, if a company wishes to expand into a new geographic area or product line, it may seek a list of potential customers from a third party. Under *opt-out*, a third party is free to provide the company with such a list, provided that it excludes consumers who have already opted-out of receiving such communications. The company can then use the list to contact people with a special offer or introductory discount. After receiving the offer, consumers are free to opt-out of receiving future offers from that company. The only "harm" suffered by the individual is receiving an offer in which he or she ultimately was not interested.

Under *opt-in*, every person on that list will need to be contacted for consent. The company *cannot* contact them, because it does riot have explicit consent to make such a use of their names or addresses. The third party supplying the list is unlikely to bear the expense and inconvenience of contacting every person on the list. The promise of explicit consent in the opt-in requirement has resulted in nothing to consent to at all.

Alternatively, depending upon the specific requirements of the opt-in law, the new service provider may be allowed to contact potential customers, but it will have to do so twice: once to gain consent to make the second contact conveying the offer. Moreover, since most requests for consent are ignored, the most likely effect on an opt-in law is to prevent contacting potential customers entirely. This is why Robert E. Litan, Director of the Economic Studies Program and Vice President of The Brookings Institution, has written that switching from an opt-out system to an opt-in system would "raise barriers to entry by smaller, and often more innovative, firms and organizations."[17]

OPT-IN AND THE ILLUSION OF CONSENT

Because of the inherent difficulty of businesses contacting consumers individually, many consumers may miss out on opportunities that they would value, not because they chose not to receive them, but because they *never had the opportunity to choose*. In one-third of households called by U.S. West, for example, the company *never reached the customer*, despite repeated attempts. Consequently, those customers were denied the opportunity to receive information about new products and services.[18] This is a very practical example of the way in which an opt-in system may only create the *illusion* of consent.

We have already seen the extent to which consumers ignore requests for consent. Moreover, even when mail is actually read and the offer appeals to the consumer, lethargy and the competing demands of busy lives often conspire to ensure that no action is taken. Only 6–11 percent of customers in the U.S. West opt-in test responded to written opt-in requests, even though more than four times that number—28 percent—indicated that they desired the service when called about it, and, as noted, 72 percent ordered the service when asked during a phone call that the customer initiated.[19] This suggests that the issue isn't privacy or the attractiveness of the request, but rather the annoyance to consumers of being interrupted with requests for consent—precisely what an opt-in law contemplates.

The opportunity to consent may also be illusory because the business wishing to use the information has no affordable way of reaching consumers individually. If the cost of obtaining consent is too great to make the proposed use of information economically feasible, then there will be nothing to which the consumer can consent.

If opt-in means that lists of potential customers are no longer available from third parties, then, as we have seen, the promise of explicit consent in the opt-in require-

ment will likely result in nothing to consent to at all. Consider the example of AOL Time Warner. As a startup company, AOL mailed free copies of its software to people likely to be interested in Internet access. Prohibiting the fledgling AOL access to information about consumer addresses and computer ownership would have denied consumers information about an opportunity that many of them obviously value, increased the volume of marketing material that AOL would have been required to distribute, and threatened the financial viability of a valuable, innovative service.

The opportunity for consent under an opt-in system may also be illusory because of the difficulty of building new data systems, and implementing new uses of data, one customer at a time. For example, highly valued services, such as consolidated statements and customer service, could not exist if consumers were given the choice about the sharing of information about their accounts, because few businesses could realistically provide both consolidated and nonconsolidated services. To do so would require one customer service center manned by one set of representatives using one information system for customers who consented to information-sharing, and a panoply of other customer service centers manned by teams of other representatives using a variety of other information systems each covering only a single aspect of a customer's account for those customers who did not consent. This is an area where there is *no* room for consumer choice—opt-in or opt-out: Service must either be provided on a consolidated basis for all (which is the choice of most consumers) or for none (in which cases all customers must endure the added cost and inconvenience of separate statements and service centers).

Finally, as noted, the opportunity for consent is always illusory if the service or product *cannot* or *will not* be provided without personal information. I experienced a very practical example of this just this past weekend. When downloading software, I was presented with a pop-up privacy policy. I could not continue installing the software I wanted without providing the information requested—the site needed to know certain information about my system to know which software to send and how to configure it—and without clicking on the "I accept" button. The presence of that policy was a small burden and annoyance, but yielded no benefit. *The opportunity to opt in meant nothing—was wholly illusory—because consent was a condition of service.* A law requiring opt-in consent in that situation would have merely increased the cost and burden of formally verifying and recording the consent that I had already manifest by my behavior, to use information without which the requested service could not have been provided.

THE LESSON FROM EUROPE

A number of legislators and privacy advocates have argued that since the use of personal information in Europe is conditioned on opt-in consent, the burdens and costs of opt-in must not be as great as research and experience have suggested. This argument is fundamentally flawed, as we are learning.

While it is true that European nations are required under the European Union data protection directive, which took effect in 1998, to condition the collection, use, or transfer of personal information on explicit opt-in consent,[20] there is little evidence that any have, in fact, done so. European data protection officials have repeatedly pointed out the impossibility of doing so. Instead, Europe has used a concept of "implied explicit consent"—if individuals are told of the intended data collection or use and do not object, then surely, European data protection officials argue, they must have opted-in. There is nothing to distinguish this from opt-out. Privacy scholar Amitai Etzioni has noted that European citizens rarely, if ever, are asked for explicit permission to use personal information about them. In fact, he tells of regularly asking his European audiences if anyone has ever been asked to opt-in. To date, Etzioni reports only one positive response-from a man who was asked for opt-in consent by Amazon.com, a U.S. company.[21] "It seems that this EU directive is one of those laws that is enacted to keep one group—privacy advocates and their followers—happy and, as a rule, is not enforced so that commerce and life can continue."[22]

A January 2001 study by Consumers International bears out Etzioni's conclusion. Consumers International examined the use and protection of personal information on 751 retail, financial, health, and other popular Web sites in the United States and Europe. The study found that while U.S. and European Web sites collect personal information at nearly comparable rates (66 percent in the United States; 63 percent in Europe), U.S. sites provide better privacy protection, despite having no specific legal obligation to do so, than European sites, which are subject to comprehensive legal requirements:

> Despite tight EU legislation in this area, researchers did not find that sites based in the EU gave better information or a higher degree of choice to their users than sites based in the US. *Indeed, US-based sites tended to set 'the standard for decent privacy policies.*[23]

Ironically, not only have more restrictive laws failed to provide a higher standard of privacy protection, they have also failed to quell consumer fears. Polls on consumer privacy concerns show nearly identical results in the United States and Europe, despite wide differences between laws. For example, Lou Harris & Associates found in 1999 that 80 percent of U.S. consumers and 79 percent of German consumers surveyed agreed with the statement "consumers have lost all control over how personal information is collected and used by companies."[24] Similarly, 71 percent of the U.S. sample and 70 percent o0 of the German sample agreed that "it is impossible to protect consumer privacy in the computer age."[25] In fact, despite the far greater legal protections for privacy available in Europe, Americans (64 percent) were more likely than Germans (55 percent) or British (58 percent) respondents to believe that businesses will handle personal information in a "proper and confidential way."[26] However, Americans (29 percent) proved no more likely than Germans (28 percent) and only slightly more likely than the British (23 percent) to say they personally have been a victim of what they. felt was an improper invasion of privacy by a business.[27]

OPT-IN AND THE FIRST AMENDMENT

Opt-in also poses significant constitutional issues under the First Amendment. The Supreme Court has struck down many ordinances that would require affirmative consent before receiving door-to-door solicitations,[28] before receiving Communist literature,[29] even before receiving "patently offensive" cable programming.[30] The Court's opinion in the 1943 case of *Martin* v. *Struthers—involving a local ordinance that banned door-to-door solicitations without explicit (opt-in) householder consent—is particularly apt:*

> Whether such visiting shall be permitted has in general been deemed to depend upon the will of the individual master of each household, and not upon the determination of the community. In the instant case, the city of Struthers, Ohio, has attempted to make this decision for all its inhabitants.[31]

The only Federal court to review a modern opt-in requirement concluded that it violated the First Amendment. In 1999, the U.S. Court of Appeals for the Tenth Circuit in *U.S. West, Inc.* v. *Federal Communications Commission*, struck down the Commission's rules requiring that telephone companies obtain explicit consent from their customers before using data about those customers' calling patterns to market products or services to them.[32] The court found that the FCC's rules, by limiting the use of personal information when communicating with customers, restricted U.S. West's speech and therefore were subject to First Amendment review. The court determined that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a *"specific and significant harm"* on individuals, and that the rules were "'no more extensive than necessary to serve [the stated] interests."'[33]

> Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial State interest under *Central Hudson* [the test applicable to commercial speech] for it is'not based on an identified harm.[34]

The court found that for the Commission to demonstrate that the opt-in rules were sufficiently narrowly tailored, it must prove that less restrictive opt-out rules would not offer sufficient privacy protection:

> Even assuming that telecommunications customers value the privacy of [information about their use of the telephone], the FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. *Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech, jurisprudence requires.*[35]

The court found that the FCC had failed to show why more burdensome opt-in rules were necessary, and therefore struck down the rules as unconstitutional. The Supreme Court declined to review the case.[36]

The Tenth Circuit's opinion in *U.S. West* is particularly applicable to the current debate over opt-out and opt-in because it reaffirms what the Supreme Court had previously indicated: that opt-in is more burdensome than opt-out, and that, as a result, for the government to adopt opt-in rules, it must first demonstrate that opt-out is not adequate.

CONCLUSION

The Role of Opt-In

Opt-in has its place. For example, Congress wisely required the explicit consent of parents before Web sites collected information from very young children.[37] Information that is particularly sensitive or particularly likely to be misused to harm the individual might also be subjected to opt-in consent. And some companies online today voluntarily use opt-in in settings where it is most easily managed (such as online service providers, which by definition have contact with their customers every time they log on) or where it is necessary to ensure consumer confidence given the sensitivity of the relationship and information (such as certain financial and health sites). But in other settings, the higher costs imposed by a legally mandated opt-in system are unwarranted.

This is especially true on the Internet where much of the information disclosed is not sensitive or likely to be used to harm the individual, but rather is a substitute for the very address information browsing and buying habits that store clerks and merchants have been noting for years. Moreover, because the use of information is so central to customer service and convenience online, and the very attraction of the Internet is its speed and ease-of-use, opt-in as a legal requirement seems peculiarly inappropriate in the context of the Internet.

Opt-in is unlikely to enhance privacy protection, because consumers asked to opt in prior to receiving service are likely to do so to receive service and to avoid the annoyance of being asked again. (That is why millions of us click "I accept" boxes without ever reading the terms to which we are agreeing.) Consumers asked to opt in later to new uses of information are in most settings unlikely to ever be aware of the request. This suggests that simply conditioning the use of personal information on specific consent is tantamount to either creating a hoop that Web users *must* jump through to obtain access to the information and services they desire, or, alternatively, to effectively *prohibiting outright* many beneficial uses of information. In either case, opt-in acts like a *tax* on online commerce, compelling all consumers to pay for the heightened privacy concerns of a few, yet providing enhanced privacy to no one.

The Role of the Government

The fact that opt-in laws do not appear generally appropriate or necessary for protecting privacy on the Internet, does not mean that there is no role for the government or for law in protecting privacy online. Far from it.

Regulators and law enforcement officials should enforce existing privacy laws vigorously, and legislators should ensure that they have the resources to do so. This is especially important in the context of the Internet, where disparate jurisdictions and laws can make enforcing existing laws difficult for most consumers. I think it is especially important for the government to help ensure that Web sites adhere to the commitments that they make in their privacy policies—whether those policies are voluntary or required by law—so that individuals who do read those policies can rely on them with confidence.

The government should also help educate the public about privacy and the tools available to every citizen to protect our own privacy. Many privacy protections can only be used by individuals—no one else can protect their privacy for them. This is especially true on Web sites, a majority of which originate in countries outside of the United States. The common sense steps and practical technologies that individuals can employ to protect themselves offer better, more effective protection than any law. Yet few individuals will recognize the importance of their responsibility or have the knowledge to fulfill it without education.

Finally, should Congress conclude that some form of new mandated consent requirement is necessary, *opt-out* is the less burdensome alternative and the one more likely to be effective. It allows people who are most concerned about their privacy to act to protect it—using the same legal right that they have with opt-in—without unduly burdening the great majority of us who are unlikely to read or act on privacy notices. You may wish to take steps to make privacy notices more complete and clear, and opt-out more effective. I advise caution, however, before substituting Congress' judgment for that of the market. Remember, the Gramm-Leach-Bliley privacy notices that the press and State legislatures are so busy criticizing, were largely

written by Federal regulators. Their complexity is precisely what we should expect if we require those notices to comply with Federal regulations and regard them as creating binding contracts. Before mandating such notices online, I urge you to think carefully about whether there is any certain way to do better, and whether the cost of doing so is justified in light of the few consumers who will ever read them.

Thank you again for the opportunity to testify.

ENDNOTES

1. Restatement (Second) of Torts §§ 652B, D-E (1976).
2. *Philadelphia Newspaper, Inc.* v. *Hepps*, 475 U.S. 767, 777 (1986).
3. Restatement, supra, § 652E.
4. 15 U.S.C. § 1681 b(a) (1999).
5. Enactment of the Children's Online Privacy Protection Act, 106th Congress, 2d Session, 146 Cong. Rec. E616, May 2, 2000, statement of Jay Inslee (D-Wash.) (emphasis added).
6. Democrats Hold News Conference on Financial Privacy, May 4, 2000 (statement of John LaFalce (DN.Y.)) (emphasis added).
7. National Association of Attorneys General, supra at 7 (emphasis added).
8. S. 30, 107th Cong. § 2 (2001); H.R. 89, 107th Cong. § 2(b)(1) (2001); H.R. 347, 107th Cong. § 2(b)(1)(A) (2001) (emphasis added)
9. "Briefs," Circulation Management, May 1999 (referring to the U.S. Postal Service's Household Diary Study (1997)).
10. Federal Trade Commission, Workshop on The Information Marketplace: Merging and Exchanging Consumer Data, Mar. 31, 2001 (comments of Ted Wham).
11. Less than 3 percent of the U.S. population takes advantage of the Direct Marketing Association's Mail and Telephone Preference Services. Financial Privacy, Hearings before the Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services, House of Representatives, 106th Cong., 1st Sess. (July 20, 1999) (statement of Richard A. Barton) (available at *http://www.house.gov/banking/72099rba.htm).* Financial institutions, retailers, and other businesses report similar or lower figures for their opt-out programs.
12. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress* at 11 (2000).
13. Brief for Petitioner and Interveners at 15–16, *U.S. West, Inc.* v. *Federal Communications Commission*, 182 F.3d 1224, 1239 (10th Cir. 1999) (No. 98–9518), cert. denied 528 U.S. 1188 (2000).
14. Ernst & Young LLP, *Customer Benefits from Current Information Sharing by Financial Services Companies* 16 (Dec. 2000).
15. Id.
16. *U.S. West, Inc.* v. *Federal Communications Commission*, 182 F.3d 1224, 1239 (10th Cir. 1999), cert. denied 528 U.S. 1188 (2000).
17. Robert E. Litan, Balancing Costs and Benefits of New Privacy Mandates, in Lucien Rapp & Fred H. Cate, *European and U.S. Perspectives on Information Privacy* (forthcoming).
18. Brief for Petitioner and Interveners at 15–16, *U.S. West*, supra.
19. *U.S. West*, 182 F.3d at 1239.
20. Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data art. 7 (Eur. O.J. 95/L281).
21. Personal communication from Amitai Etzioni to the author (Feb. 21, 2001).
22. Amitai Etzioni, "Protecting Privacy," *Financial Times*, April 9, 1999, at 18.
23. Consumers International, *Privacy@net: An International Comparative Study of Consumer Privacy on the Internet* at 6 (2001) (emphasis added).
24. *IBM Multi-National Consumer Privacy Survey* at 22 (1999).
25. Id.
26. Id.
27. Id. at 14.
28. *Martin* v. *Struthers*, 319 U.S. 141 (1943).
29. *Lamont* v. *Postmaster General*, 381 U.S. 301 (1965).
30. *Denver Area Educational Telecommunications Consortium, Inc.* v. *Federal Communications Commission*, 518 U.S. 727 (1996).
31. *Martin*, 319 U.S. at 14 1.
32. *U.S. West*, 182 F.3d at 1235.
33. Id. at 1235 (quoting *Rubin* v. *Coors Brewing Co.*, 514 U.S. 476, 486 (1995)).
34. *U.S. West*, 182 F.3d at 1235 (emphasis added).
35. Id. (emphasis added).

36. *U.S. West Communications, Inc.* v. *Federal Communications Commission*, 528 U.S. 1188 (2000).
37. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105–277, 112 Stat. 2681–728 (codified as amended at 15 U.S.C. § 6501–06 (1999)).

The CHAIRMAN. Thank you very much.

Just a moment, Dr. Schwartz. Senator Burns, our ranking member on communications has to be at the Interior Appropriations Subcommittee markup.

Senator Burns, you had a statement?

STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. Well, I have a statement, and I would ask unanimous consent that that statement might be just entered in the record, Mr. Chairman. I thank you for this courtesy. And, of course, Senator Wyden and I will still be very much involved in this issue with our bill, and we look forward to working with you and the rest of the Committee as this legislation moves forward. And I thank you for the courtesy.

The CHAIRMAN. Very much thank you.

[The prepared statement of Senator Burns follows:]

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Thank you, Mr. Chairman. Today's hearing concerns a topic of crucial importance in today's increasingly digital world: the protection of online privacy.

To put it simply, Americans have no safety net of privacy online. Ever-more sophisticated technologies are being developed to collect nearly limitless information on individuals without their knowledge. Consumers are clearly concerned at the "flip side" of the digital revolution. Just yesterday, the Markle Foundation released a landmark report on the "State of the Net" which revealed that nearly half of the public viewed the Internet as a "source of worry." Foremost among their concerns is the lack of privacy on the Internet. A recent Gallup poll found that nearly four-fifths of Americans were concerned about the privacy of personal information they give out on the Internet. Seven in ten online shoppers were concerned about the security of their information. In addition, two-thirds of those polled called for Federal legislation to protect their online privacy.

None of these striking numbers surprise me, as I continue to hear from my contituents about the lack of privacy protections on the Internet. I am more convinced than ever that legislation is necessary to provide consumers with a safety net of privacy in the online world.

Online privacy is central to the future economic well-being of the Internet. Despite the recent highly publicized flameouts of several dot-com companies, e-commerce has continued to grow. However, the rate of this growth is clearly being slowed by consumers' rising and legitimate fears about privacy intrusion. Several studies pointed out that the primary reason preventing more people from making purchases online is the lack of privacy. While the Internet has exhibited massive growth, currently less than 1 percent of all consumer retail spending is done online. In short, e-commerce still has huge upside potential, but that potential will never be fulfilled without basic assurances of consumer privacy.

I would like to touch on the idea that merely posting privacy policies somehow ensures actual privacy for users. Many of these policies are frustrating exercises in legalese. It becomes obvious from wading through examples of these policies that most were designed with the goal of protecting companies from liability rather than informing and empowering consumers. In today's hectic world, consumers simply don't have either the time or the inclination to slog through confusing policies that span multiple pages.

To address these concerns, in the 106th Congress, Senator Wyden and I introduced the "Online Privacy Protection Act," which was based on our shared view that while self-regulation should be encouraged, we need to also provide strong enforcement mechanisms to punish bad actors.

I am open to working with the Chairman, Sen. Wyden and all of my colleagues on the Committee to ensure that strong privacy legislation moves to markup and

passage by the full Senate as quickly as possible. I look forward to the testimony of the witnesses. Thank you.

The CHAIRMAN. Dr. Schwartz.

STATEMENT OF PAUL M. SCHWARTZ, PROFESSOR OF LAW, BROOKLYN LAW SCHOOL

Mr. SCHWARTZ. Thank you. I am honored to be here today to talk about Internet privacy with you.

Millions of Americans now engage in daily activities on the Internet. Under current conditions, their behavior, our behavior, creates detailed stores of personal data. The key concept is that the Internet is an interactive telecommunications system. In other words, computers attached to it do not merely receive information but also transmit it. Visits to the Internet create data trails.

What I would like to do today is briefly make three points. First, I wish to address the EU data protection directive and the U.S. Commerce Department's safe harbor agreement. Second, I wish to talk about weaknesses in the current market for online privacy. Third and finally, I wish to describe the nature of the privacy harms to individuals in the online realm. Let me begin.

The European data protection directive seeks to harmonize privacy law in Europe at a high level. It also restricts transfers of information to third-party nations that lack an adequate level of protection. The response of the U.S. Commerce Department has been to draft and negotiate EU approval of safe harbor standards for privacy. And what does the safe harbor provide? They provide the fair information practices that Senator McCain alluded to in his opening statement: notice, choice, access, security, and enforcement.

After a slow start for the safe harbor, more American companies are signing up for it. Chairman Hollings in his opening statement spoke of the number of leading information age companies that have signed on to the safe harbor. In my judgment, it speaks well for the business compatibility of the safe harbor that companies such as Intel, Hewlett-Packard, Acxiom Data and Microsoft have agreed to it.

The thing to remember, though, is that the EU directive is there only to protect European citizens. It creates legal obligations only for their information. The resulting gap in protection leaves American citizens entitled under law only to a lesser level of privacy protection.

Let me now turn to my second topic. In my view, we do not have a well-functioning privacy market. What would a well-functioning market require? It would require consumers who want to sell or exchange their information to be able to bargain over the terms under which they disclosed their personal data. It would also require data processors, the buyers of information, to offer different packages and prices for personal information.

Currently, however, what we have on the Internet is a Hobson's choice. Now, the original Hobson was an innkeeper in England in the 17th Century. Hobson told his customers that they were to take the horse closest to the stable door or they would take no horse in the stable. That was the original Hobson's choice. The Hobson's choice that we are now seeing is either no privacy or no Internet,

and I think this is exactly what Senator Rockefeller pointed to when he talked about the problems with cookies. It is, in fact, very, very difficult to manage cookies.

Even beyond cookies, we have problems such as "web bugs", also known as clear GIF's and many other privacy meltdowns that are only a click stream away. So the emerging Hobson's choice for Americans on the Internet is to sacrifice either privacy or access to the Internet.

I now reach my third and final point. Let me try to describe a way of thinking about the kinds of harms that occur to privacy on the Internet. In my judgment, we have both economic and noneconomic harms. The first economic harm is a distributional one. The failure in the privacy market involves a distribution away from consumers who care about privacy and toward data processing companies. In other words, we have a subsidy to data processing companies. They are essentially getting information, our information, at a below true market rate.

The second problem is weblining. Weblining is an emerging practice on the Internet which is similar to "redlining" in the off-line world. Weblining creates segmenting in which it is our data profiles that decide the price that we pay, the services we obtain, and our access to new products and information. The danger is that weblining will hinder the kind of increased opportunity that access to information should provide.

The third economic harm on the Internet is a deadweight cost. Consumers are buying less or not buying at all because of their worries about privacy. In a November 2000 report, the Forrester Research Group found that such consumer concern led U.S. companies to have $12.4 billion in lost sales in the year 2000 alone.

Finally, there are noneconomic harms. Cyberspace is not only a place for shopping; it is our new arena for public and private activities. Yet, as Professor Jerry Kang of UCLA Law School has written of cyberspace, it is a place where you are invisibly stamped with a bar code. In the absence of strong privacy rules, Americans will hesitate to engage in cyberspace activities, including those that are most likely to promote community.

Allow me to conclude. It is my hope that the Senate Commerce Committee will respond to the situation I have described with introduction of strong consumer privacy legislation. Thank you for the opportunity to testify.

[The prepared statement of Mr. Schwartz follows:]

PREPARED STATEMENT OF PAUL M. SCHWARTZ, PROFESSOR OF LAW, BROOKLYN LAW SCHOOL

Mr. Chairman and Members of the Committee: My name is Paul Schwartz, and I am a Professor of Law at Brooklyn Law School in Brooklyn, New York. For over a decade, I have been writing and teaching about privacy law and other areas of information law. My publications about privacy law include two co-authored reports carried out at the request of the Commission of the European Union. I have also taught courses in areas such as privacy law, Internet law, telecommunications law, and the "Law of Electronic Democracy."

Millions of Americans now engage in daily activities on the Internet, and under current technical configurations, their behavior—our behavior—creates detailed stores of personal data. The Internet is an interactive telecommunications system, which means that computers attached to it do not merely receive information but also transmit it. Social, political and commercial life on the Internet create a finely grained data map of our interests, our beliefs, and our interpersonal relationships.

This personal information also has great commercial value; it is no exaggeration to consider personal data to be the gold currency of the Information Age.

It is, therefore, fitting that the Senate Commerce Committee is examining Internet privacy. I am honored to be here today to share my views regarding privacy law in cyberspace.

There are three topics that I wish to address: (1) the European Data Protection Directive and the Safe Harbor Agreement; (2) the weaknesses in the current "market" for online privacy (the problem of "privacy market" failure); and, finally, (3) the nature of the privacy harms that individuals currently suffer in the online realm.

I. THE EUROPEAN DATA PROTECTION DIRECTIVE

The Member States of the European Union (E.U.) have enacted a Data Protection Directive that seeks both to harmonize their national data protection laws at a high level and to restrict transfers of personal data to third-party nations that lack "an adequate level of protection."[1] In cases where such adequate protection is not present, the Directive provides exceptions that permit transfers if, among other circumstances, the party receiving the data has agreed by contract to provide adequate protection.[2]

These national and European-wide measures for information privacy pose significant challenges to the free flow of personal data to the United States. Whether or not a U.S. company has "adequate" measures for information privacy requires examination of the protections available for specific data, including the safeguards offered by law and relevant business practices.[3] As a general matter, the European view regarding United States privacy law has been skeptical.[4]

In response to E.U. Data Protection Directive, the U.S. Commerce Department drafted and negotiated E.U. approval of "Safe Harbor" standards for privacy.[5] The Commerce Department sought to bridge differences in privacy approaches between the two countries and to "provide a streamlined means for U.S. organizations to comply with the Directive."[6] As the Commerce Department states, "The safe harbor—approved by the EU in July of 2000—is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws."[7] Under Ambassador David Aaron's leadership, the Commerce Department also obtained E.U. agreement to waive sanctions against any American companies that follow these standards. American companies in the Safe Harbor are deemed to provide "adequate protection" for the personal data of Europeans.

What does the Safe Harbor provide? Americans companies that sign up for it promise to provide a range of Fair Information Practices for the personal information of Europeans. Fair Information Practices are the building blocks of modern information privacy law; they are centered around four key principles: (1) defined obligations that limit the use of personal data; (2) transparent, that is open and understandable, processing systems; (3) limited procedural and substantive rights; and (4) external oversight.[8] These principles are not a European invention, but have been present in information privacy law and policy in the U.S. since the era of mainframe computers in the 1970's.

After a slow start for the Safe Harbor, more American companies are signing up for it. Perhaps the single most exciting development in the last year in U.S. privacy law has been this new willingness of corporate America to pledge allegiance to the most important Fair Information practices. Among the corporations now on the Safe Harbor list are Intel, Hewlett Packard, and Acxiom Data. Moreover, Microsoft has announced that it plans to sign on to the Safe Harbor agreement. These are, of course, all leading Information Technology corporations, and Acxiom is also a leading collector of personal data. Based in Little Rock, Arkansas, Acxiom Data supplies data infrastructure and technology services to help companies and organizations better understand customer behavior. It speaks well for the business compatibility of the Safe Harbor that these companies have agreed to it.

Under the terms of the Safe Harbor, however, American companies pledge to provide Fair Information Practices only for the personal data of European citizens. The question then becomes: why should American citizens be entitled under law only to a lesser level of privacy protection?

II. WEAKNESS IN THE CURRENT PRIVACY MARKET

In this part of my testimony, I wish to consider the foundation conditions for a functioning "privacy market" and to explore the weaknesses in the existing market for personal information.

A well-functioning privacy market requires sellers (i.e. consumers) to be able to bargain over the terms under which they will disclose their personal data, and buy-

ers (i.e. data processors) to offer different packages and prices for this personal information. In such a market, "privacy price discrimination" will emerge. Privacy price discrimination involves a consumer seeking different packages of services, products, and money in exchange for her personal data, and a data processing company differentiating among consumers based both on their varying preferences about the use of their personal data and the underlying value of the information.

To illustrate this point, imagine two hypothetical consumers: Marc and Katie. Marc cares deeply about how his personal information is used; Katie does not. A surplus from cooperation under a property regime requires at a minimum, however, that Marc and others with similar preferences receive more than their "threat value" before disclosure. The term "threat value" refers to the "price" that Marc would place on *not* disclosing his personal information. Beyond receiving the threat value, privacy price discrimination also requires further elasticity in meeting more subtle privacy preferences of Marc. Under the current regime, however, companies generally have no need to offer Marc greater services or more money for his personal data than they offer Katie.

The failure in the privacy market can be attributed to at least four causes: (1) information asymmetries; (2) collective action problems; (3) bounded rationality; and (4) limits on "exit" from certain practices. We should briefly consider each of these four shortcomings in the privacy market.

A. Information Asymmetries

The first weakness in the privacy market is that most visitors to cyberspace lack essential knowledge of how their personal information will be processed or how technology will affect data collection. Due to this "knowledge gap," development through a privacy marketplace of rules for personal data use are likely to favor the entities with superior knowledge—online industry rather than consumers. At present, even relatively basic Internet privacy issues, such as "cookies," are met with widespread consumer ignorance.

Cookies are alphanumerical files that Web sites place on the hard drives of their visitors' computers. Cookies are a ready source of detailed information about personal online habits, but consumers generally do not even know where cookie files are stored on their computer. Beyond cookies, widespread information asymmetries involve other aspects of the Internet's technical infrastructure. As a result, "negotiations" about the use of personal information occur with one party, the consumer, generally unaware that bargaining is even taking place!

B. The Collective Action Problem

The second difficulty in the Internet privacy market is a collective action problem. The need is for individual privacy wishes to be felt collectively in the market. The good news first: a group of privacy-promoting organizations are emerging. Among these institutions are: (1) industry organizations that support self-regulation by drafting codes of conduct; (2) privacy seal organizations, such as TrustE and BBBOnline; (3) "infomediaries" that represent consumers by offering to exchange their data only with approved firms; (4) privacy watchdog organizations that bring developing issues to public attention; and (5) technical bodies, such as the World Wide Web Consortium (W3C), engaged in drafting Internet transmission standards, including the Platform for Privacy Preferences (P3P). P3P is a software transmission protocol that seeks to allow the individual to control her access to Web sites based on her privacy preferences and the practices at a given site.

Despite these promising developments, most of us are not yet able to free-ride successfully on the efforts of those who are more savvy about data privacy on the Internet. As many experts have pointed out, current collective solutions, such as industry self-regulation and privacy seals, are flawed. As an example, the FTC's 2000 Study, *Privacy Online*, points to the lack of effective enforcement in current models of industry self-regulation and the confusing implementation of privacy seal programs.[9] For that matter, the existence of competing privacy seal programs raises the risk of forum shopping by Web sites that are hoping for weaker enforcement from one seal service rather than the other.

C. Bounded Rationality

The third difficulty with the privacy market is "bounded rationality," a concept developed by behavior economists.[10] Scholarship in behavioral economics has demonstrated that consumers' general inertia towards default terms is a strong and pervasive limitation on free choice. This does not mean that consumers are all sheep, but it does mean that default rules and form terms can have great psychological force and are likely to reward those who otherwise have greater power.

As a result of this current power dynamic, individuals faced with standardized terms and expected to fend for themselves with available technology may simply ac-

cept whatever terms are offered by data processors. Indeed, the difficulties with bounded rationality extend not only to personal information as traditionally understood but a new and potentially risky set of personal information, namely "privacy meta-data." This point is worth elaborating.

Meta-data are information about information. For example, use of telecommunications now creates "communications attributes," which are valuable data about consumers' service and calling preferences (call waiting, caller ID, DSL lines, etc.). The use of privacy filtering technology, such as P3P, creates another kind of meta-data, namely information about one's privacy preferences. Ironically, these meta-data will possibly contribute to additional privacy invasions. Already in the offline world, direct marketers generate and sell lists of people who have interest in protecting their privacy. *Filtering will therefore create the possibility of further privacy violations unless customers prove able not only to negotiate for their privacy but for the privacy of data about their privacy preferences.*

Bounded rationality points to the need to find ways to permit informed decision-making about use of one's personal information and personal meta-information at the least cost to a consumer. The risk is that the current privacy market will lead only to cyber-agreements that represent new kinds of contracts of adhesion. In other words, new technology may lead only to speedy ways to generate poor contracts.

D. Limits on Exit

Finally, cyberspace, in certain of its applications, turns out to be far from friction-free. In particular, when limits exist on "exit" from certain practices, the danger is that online industry will be able to "lock-in" a poor level of privacy on the Web. Again, cookies provide a good example—cookies demonstrate how privacy "lock-in" takes place. A ready source of detailed information about personal online habits and in widespread use, cookies are difficult to combat. Mastery of advanced settings on one's Web browser, the downloading of "cookie-cutting" software, and some public protests about more egregious practices have helped, but not solved this problem. As a joint paper of the Electronic Privacy and Information Center (EPIC) and Junkbusters has noted, "Those consumers, who have taken the time to configure their browsers to notify when receiving, or reject cookies, have found that web surfing becomes nearly impossible." [11]

Moreover, beyond cookies, the next privacy melt-down is never far away. A possible source for the next crisis are so-called "Web bugs," also known as "clear GIF," which permit Web sites to snoop on visitors by use of code that occupies only one pixel on the screen. To return to my earlier point about information asymmetries, an even lower level of consumer awareness exists about Web bugs than about cookies.

As a final example of the emerging "lock in" for informational privacy, many of us enter cyberspace anchored in real space settings that limit our ability to negotiate. The modern workplace demonstrates this phenomenon. As the *New York Times* concludes, "the debate over employee privacy is over." [12] It is over because "widespread, routine snooping on employees is no longer a threat but a fact." [13] Or, as *Business Week* states, "When it comes to privacy in the workplace, you don't have any." [14] The emerging Hobson's choice for Americans on the Internet is to sacrifice either privacy or access to the Internet.

Let us conclude this section by returning to Marc and Katie, our two consumers with different privacy preferences. Due to the pervasive failure in the privacy market in the United States, commercial entities generally obtain Marc's and Katie's personal data for the same low price. As a result, a subsidy is given to those data processing companies that exploit personal data. Put simply, the true "cost" of personal data is not charged these organizations. One likely result of subsidized personal information is that companies will over-invest in reaching consumers who do not wish to hear from them. Personal information at below-market costs will also lead companies to under-invest in technology that will enhance the expression of one's privacy preferences.

III. ECONOMIC AND NON-ECONOMIC HARMS CAUSED BY PRIVACY VIOLATIONS

It may be difficult at times to understand the nature of privacy harms that occur in cyberspace. And it is certainly true, as Professor Fred Cate and others have reminded us, that benefits are associated with the sharing of information.[15] Why should there be limits on the use of personal data? In my view, the nature of the harms to personal privacy on the Internet fall into two categories: (1) the economic, and (2) the non-economic.

A. Economic Harms

Privacy violations cause economic harms to consumers by: (1) causing an exchange of our personal information at lower rates than a fully functioning privacy market would permit; and (2) squelching democratic opportunity through emerging practices such as "Weblining." Finally, privacy violations also lead to: (3) a lack of consumer confidence that harms the development of e-commerce.

1. Personal Data at Below "Market" Rates

I have proposed that the true cost of personal data is not imposed on organizations—the personal data of consumers (the Marc's) who care about privacy and those that do not (the Katie's) can be obtained for the same price. This market failure leads to both deadweight losses and distributional consequences. The deadweight losses follow from the existence of consumers who would engage in more or different kinds of transactions on the Internet, but refuse to do so because of fears about how their personal data will be collected and used. Polls have consistently shown that many Americans decline to engage in cyberspace transactions because of such worries.[16] In this fashion, a deadweight loss reduces the economic surplus that would be created were privacy price discrimination in place. Such a loss, perhaps somewhat hidden during the Internet's early stages of rapid growth, will become more visible as e-commerce enters a slower stage. As a columnist in Silicon Valley's *Mercury Center* warns, "almost all of the online retailers hurriedly launched in 1998 and 1999 now appear doomed to disappear—not because e-commerce isn't going to be important, but because consumers aren't moving fast enough toward online shopping to sustain today's Web retailers."[17]

The failure in the privacy market also involves a distribution away from Marc and even Katie and towards data processing companies. Companies have no need to offer Marc greater services or more money for his personal data. In fact, they may not even meet Katie's more modest privacy threat value.

2. Weblining and the Limiting of Opportunity

The benefits of access to information, including personal information, can certainly be positive. Yet, the processing of personal data can also create significant social risks. If used improperly, profiling will squelch opportunity rather than promote it. Consider the emerging practice of "Weblining," which is similar to "red-lining" in the real world. Weblining, as *Business Week* tells us, is the "Information Age version of that nasty old practice of redlining, where lenders and other businesses mark whole neighborhoods off-limits."[18] Weblining sews far-flung threads of personal data, including data about one's ethnic background or religion, into profiles that are used to sort people into categories and predict how they will behave. It creates segmenting in which it is our data profiles that decide the price that we pay, the services we obtain, and our access to new products and information. Weblining sometimes even relies on so-called "neural networks," which are digital systems that evolve over time in a fashion both independent of their developers and impossible to predict.

The danger is that Weblining will hinder or even reverse the kind of increased opportunity that access to information can stimulate. It can be used to limit economic and informational possibilities for individuals and different groups in a fashion that reflects and reinforces existing prejudices and mistaken beliefs. As *Business Week* warns, "Weblining may permanently close doors to you or your business."[19]

3. Consumer Uncertainty Harms the Development of E-Commerce

Americans may not fully understand the fashion in which Internet snooping occurs, but they do have a growing awareness that a privacy problem exists in cyberspace. As I have already noted above regarding the resulting deadweight losses, consumer worries about privacy are inhibiting electronic commerce. I wish to expand briefly on this point.

The Pew Research Center's "Internet and American Life" project furnishes insights into the dynamic of how the lack of Internet privacy harms e-commerce. The Pew Center's Internet Life Report, *Trust and Privacy Online* (August 20, 2000) found, first, that the leading fear of Internet users concerned their privacy. According to this survey, eighty-four percent of Internet users were worried about "[b]usinesses and people you don't know getting personal information about you and your family."[20] The Pew Research Center's report also noted that "[a] strong sense of distrust shades many Internet users view of the online world and the uneasiness has grown in the past two years."[21]

The Pew Research Center identified a relation between fears about privacy and "lower participation in some online activities, especially commercial and social activities."[22] In similar terms, a *Business Week*/Harris Poll from March 2000 found

a high level of concern about privacy from people who have gone online but not yet shopped there.[23] Finally, the Forrester Research Group found in late 1999 that privacy concerns had led to $2.8 billion in lost sales that year alone.[24] Uncertainty about privacy is harming the development of e-commerce.

B. Non-Economic Harms

In addition to the economic harms that follow from the lack of strong privacy standards on the Internet, non-economic harms also take place. Cyberspace is not only a place for shopping; it is our new arena for public and private activities. Cyberspace demonstrates information technology's great promise: to form new links between people and to marshall these connections to increase collaboration in political and other activities that promote democratic community. In particular, cyberspace has a tremendous potential to revitalize democratic self-governance at a time when a declining level of participation in communal life endangers civil society in the United States.

Consider the Supreme Court's decision in 1997 in *ACLU* v. *Reno*.[25] In striking down certain provisions of the Communication Decency Act, the Supreme Court declared its intention to protect the "vast democratic fora" of the Internet.[26] The Supreme Court considered the Internet to be a speaker's paradise; as the Court noted, "this dynamic, multifacted category of communication" permits "any person with a phone line" to "become a town crier with a voice that resonates farther than it could from any soapbox."[27] This language is similar to language used by the political scientist Benjamin Barber, who has defined civil society as the free space in which democratic attitudes are cultivated and conditioned.[28] In Professor Barber's words, "The public needs its town square."[29]

Without privacy, however, the implications of hanging out at the town square are dramatically changed. The Supreme Court's decision in *Reno* v. *ACLU* is also illustrative in this regard. The Supreme Court praised the Internet's potential for furthering free speech; for the Court, the Internet represented a "new marketplace of ideas."[30] We must note, however, a paradox in this regard: while listening to ideas offline, in Real Space, generally does not create a data trail, listening in cyberspace does. The Internet's interactive nature means that individuals on it simultaneously collect and transmit information; as a result, merely listening on the Internet becomes a speech-act. A visit to a Web site or a chat room generates a record of one's presence.

To extend the Supreme Court's metaphor, the role of town crier in cyberspace is often secretly assigned—a person can take on this role, whether or not she seeks it or knows afterwards that she has been given it. Already a leading computer handbook, the *Internet Bible*, concludes its description of the low level of privacy in cyberspace with the warning, "Think about the newsgroups you review or join—they say a lot about you."[31] If cyberspace is to be a place where democratic discourse occurs, the right kinds of rules must shape the terms and conditions under which others have access to our personal data. The issue is of the highest importance; the Internet's potential to improve democracy will be squandered unless we safeguard the kinds of information use that democratic community requires.

A poor level of privacy in cyberspace threatens the promise of the Internet: it discourages political and social participation in this new realm. As Professor Jerry Kang has written of cyberspace, it is a place where "you are invisibly stamped with a bar code."[32] In the absence of strong privacy rules, Americans will hesitate to engage in cyberspace activities—including those that are most likely to promote democratic self-rule.

CONCLUSION

The E.U. Data Protection Directive and the U.S. Commerce Department's Safe Harbor indicate a possibility of harmonizing global data flows at a high level of privacy protection. The question then becomes the kind of privacy protection that should be in place for personal data use within the U.S. In my testimony today, I have identified numerous grounds for concluding that the "privacy market," that is the market in which personal data are collected and exchanged in the U.S., will not alone produce the right level of information privacy. Finally, I have sought to identify a basic taxonomy of economic and non-economic harms occuring in the online realm. It is my hope that the Senate Commerce Committee will respond to this situation with introduction of strong consumer privacy legislation.

Thank you for the opportunity to testify today.

ENDNOTES

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Art. 25, O.J. of the European Communities, no.L281, 31 (Nov. 23, 1995) [hereinafter European Directive].
2. European Directive, at Art. 26.
3. European Directive, at Art. 25(2). *See Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, First Orientations on Transfers of Personal Data to Third Countries—Possible Ways Forward in Assessing Adequacy*, XV D/5020/97-EN final WP4 1–5 (June 26, 1997).
4. To make matters more complicated, the EU Directive's provisions on data transfers are enforced by the Member States, which makes their current views and future action critical.
5. *Int'l Trade Admin., Electronic Commerce Task Force, Safe Harbor Principles* (Nov. 4, 1998) <*http://www.ita.doc.gov/ecom/menu.htm*>.
6. U.S. Commerce Dept, *Safe Harbor Overview*, (visited July 9, 2001) <*http://www.export.gov.safeharbor/SafeHarborInfo.html*>.
7. *Id.*
8. For a description of early proposals regarding fair information practices, see *the Privacy Protection Study Commission, Personal Privacy in an Information Society 14- 15, 500–502 (1977); David Flaherty, Protecting Privacy in Surveillance Societies* 306–307 (1989). For analysis of fair information practices as the building blocks of information privacy, see Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 *Tex. L.Rev*. 56–67 (1997); Paul M. Schwartz, *Privacy and Participation*, 80 *Iowa L.Rev*. 563–564 (1995).
9. FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace* (May 2000).
10. For citations to the relevant academic literature, see Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy*, 2000 *Wisc. L. Rev*. 744, 768–69.
11. Junkbusters & the Electronic Privacy Information Center, Pretty Poor Privacy: An Assessment of P3P and Internet Privacy 6 (June 2000) <*http://www.junkbusters.com/ht/en/p3p.html*>.
12. Jeffrey L. Seglin, *As Office Snooping Grows, Who Watches the Watchers?*, N.Y. TIMES, June 18, 2000, at Bus. Sec. 4.
13. *Id.*
14. Larry Armstrong, *Someone to Watch Over You*, *Business Week*, July 10, 2000, at 189.
15. See, e.g., Fred H. Cate, *Principles of Internet Privacy*, 32 *Conn. L. Rev*. 877 (2000).
16. For a recent summary and discussion of the poll data, See *Federal Trade Commission, Privacy Online 2* (May 2000). As the FTC states, "surveys show that those consumers most concerned about threats to their privacy online are the least likely to engage in online commerce, and many consumers who have never made an online purchase identify privacy concerns as a key reason for their inaction." *Id.*
17. Mike Langberg, *Low cost net devices not about to push aside PC*, *Mercury Center*, July 14, 2000.
18. Marcia Stepanek, *Weblining*, *Bus. Wk.*, Apr. 3, 2000, at 2. (*http://www.businessweek.com/2000/00—14/b3675017.htm*>.
19. *Id.*
20. Pew Internet & American Life Project, *Trust and Privacy Online* 4 (Aug. 20, 2000).
21. *Id.* at 12.
22. *Id.* at 16.
23. *BusinessWeek/Harris Poll: A Growing Threat*, *Bus. Wk.*, Mar. 20, 2000, at 1. <*http://www.businessweek.com/2000/00—12/b3673010.htm*>.
24. *Trails of Personal Info Compromise Net Shopper's Privacy*, *USA Today*, Dec. 20, 1999.
25. 117 S.Ct. 2329 (1997).
26. *Id.* at 2434.
27. *Reno* v. *ACLU*, 117 S.Ct. 2329, 2344 (1997).
28. Benjamin Barber, *A Place for Us* 76 (1998).
29. *Id.*
30. Reno, 117 S.Ct. at 2352.
31. Brian Underdahl & Edward Willett, *Internet Bible* 247 (1998).
32. Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 *Stan. L. Rev*. 1193, 1198 (1998).

The CHAIRMAN. Thank you, Dr. Schwartz.

Senator McCain.

Senator MCCAIN. Thank you, Mr. Chairman.

Professor Schwartz, you state that polls have consistently shown that many Americans decline to engage in cyberspace transactions because of concerns about privacy. Why, if it is in the business's interest to improve privacy protections, do you think businesses aren't doing it?

Mr. SCHWARTZ. Well, I think it is for the reasons that I have described in my testimony—we don't have a well-functioning privacy market currently. I think there are a number of reasons for this market failure, one of which is a kind of collective action problem. It is difficult for all of our privacy needs to be felt collectively in the market.

My hope, by the way, Senator, is that in time the market will respond, and my view is the legislation that the Committee is discussing will create the kind of environmental shock to the existing privacy market on the Internet that will create privacy-enhancing organizations and companies.

Senator MCCAIN. Mr. Rotenberg, a report published by Consumers International in January suggested there was widespread noncompliance in Europe with the EU's privacy directive, which as we all know imposes very strict limitations on the collection, processing, storage, and disclosure of personal data, both offline and online. What do you think this says about the possible effectiveness of laws as a means of ensuring privacy protections?

Mr. ROTENBERG. Senator, the study by Consumers International focused on a very narrow issue in the area of privacy protection, and that was simply whether notices were being posted by companies that were operating on the Internet. The privacy directive in the European Union provides a great many rights and also creates institutions, such as Federal-level privacy officials that actively intervene on behalf of consumers to protect privacy interests. So I think taken as a whole, the privacy approach in Europe works fairly well, but it is certainly the case that on some of these specific matters, like the posting of privacy notices, there is always a question of compliance, and the CI report reflected this.

Senator MCCAIN. Do you believe that there are any limitations that the First Amendment may impose on our ability to legislate privacy restrictions, as opposed to countries that don't have a First Amendment?

Mr. ROTENBERG. Yes, I think there are, particularly in the areas of political speech, of course. Our very important First Amendment tradition, which sanctifies the right of people to speak even when the majority may disagree with them, weighs very heavily against any legislation by Congress. But here, of course, we are not really talking about political speech. We are talking about business practices, commercial communications, and there the Court has recognized——

Senator MCCAIN. But communications on the Internet could be——

Mr. ROTENBERG [continuing]. A different approach.

Senator MCCAIN [continuing]. Interpreted as a form of speech obviously.

Mr. ROTENBERG. Yes. And I think the Court would certainly consider the nature of the communications, as it has done in a number of recent cases. Both Fred Cate and I have discussed this issue, and there is the U.S. West case in the Tenth Circuit, where I think there was quite a bit of deference shown to commercial communications, but the more recent cases from the D.C. Circuit and the D.C. District Court suggest that courts are willing to uphold privacy regulations where the nature of the speech is purely commercial.

Senator MCCAIN. Mr. Cate, the issue of opt-in versus opt-out of any proposed legislation seems to dominate a lot of our debate and discussion. How critical is this element to this overall debate in regards to privacy?

Mr. CATE. Well, Senator, from my view, opt-in as a legislative requirement across the board on the Internet is fatal. It is a tremendous problem exactly for the reasons I outlined in my testimony. That is not to say there are no places where opt-in might not be appropriate. For example, Congress wisely requested when collecting information online from very young children, that there be opt-in consent from the parents. That seems entirely appropriate.

One problem with most online legislation, though, is that it does not make any distinctions between what most of us might consider private or sensitive information and all other information. So to use opt-in, the most restrictive possible privacy standard available to apply to all of that information, information that frankly might not be considered very private and information that could be considered private, is not only constitutionally fatal, but it also really creates an impediment without creating any benefit along with it, because it protects under opt-in information that is routinely disclosed or seen in the offline world, and this just makes no sense from a market perspective.

Senator MCCAIN. I would be glad to listen to Mr. Schwartz and Mr. Rotenberg's comments on that as well, but I think we also need to put this into context. Every time we make a phone call, it is recorded. Every time we go to Safeway and pay with a credit card, it is recorded. We are in a situation, not just on the Internet, but basically where all of our activities are recorded and are, to some degree, public property, which many of us are either oblivious to or don't care about.

But the fact is our lives now are not just confined to betrayal of privacy on the Internet. It is basically the way we conduct our communications and our transactions in our daily lives.

Go ahead, Mr. Schwartz and Mr. Rotenberg.

Mr. SCHWARTZ. Senator McCain, I absolutely agree with you about this, about your point about these new data trails that we leave, not only on the Internet but at the supermarket and making calls. What I have argued for the in the past is thinking about the right mixture of both opt-in and opt-out rules in legislation. I think the touchstone should be trying to figure out how to make privacy protection work at the least cost to consumers, including transaction costs. And in my view, that is going to require a mixture of both kinds of rules.

Senator MCCAIN. Mr. Rotenberg.

Mr. ROTENBERG. Senator, I will say that I think the opt-in approach reflects the common-sense approach that before business

makes use of your information for another purpose, it should ask your permission. And this is the sense that most people have about the use——

Senator MCCAIN. At Safeway?

Mr. ROTENBERG. Well, I think if Safeway is actually planning to sell your data, yes, and to sign up for one of those programs, in effect you are opting in. If they were to take the data—it is an interesting example, in fact. If they were to take the data from you after you had made the decision not to opt into their program, I think virtually everyone would agree that that would be a violation of your privacy, and as to the example of telephone records, toll records and content and so forth, that information is subject to Federal law, and restrictions are in place, so that you do have some confidence when you make telephone calls, that information will not be disclosed.

Senator MCCAIN. Thank you, Mr. Chairman.

The CHAIRMAN. We are alternating from side to side in order of appearance.

Senator Rockefeller.

Senator ROCKEFELLER. In following up, Mr. Rotenberg, what you just said, in fact, this morning I received a phone call from a telephone company calling center, in which they said that somebody last night had made a long distance call at great expense using my credit card in New Jersey.

Well, I have a son that goes to college in New Jersey——

[Laughter.]

Senator ROCKEFELLER [continuing]. But it was a very different area code number. And so—and partially in response to what Senator McCain is saying—this was a very classic example of my rights being protected, because if somebody has that telephone number and is using it, which is obviously the case, and was using it in a very expensive fashion—it was a rather long phone call—they said, "We think you should cancel your credit card number," which was against their business interests.

Now, obviously we are going to get another one, but there is going to be a period of time when I am not going to be using, you know, their number. And so that was an example where my privacy was specifically being protected, either because of Federal law, which you can answer, or because they desired to keep me on as a customer, because they knew that I would eventually see that there was somebody making an expensive phone call that simply had my number and had no right to have my number.

Is that a Federal law making them do that?

Mr. ROTENBERG. Well, I don't know if it is a Federal law that they contact you, but privacy laws certainly allow and anticipate that companies will need to do this. In fact, in the Federal wiretap statute, it is understood that telephone companies will from time to time listen in on telephone calls, and the reason that they do this is to assess the line quality, to measure their own service and to improve it.

Privacy laws don't operate as an obstacle to ensuring better service or enabling the detection of fraud where it is appropriate. The concern really arises when they take that information and say, "Well, maybe this would be of interest to someone else, or maybe

we should just disclose it". That is where privacy law says, "This is really not related to the delivery of that service," the performance of our business responsibilities. Here we need to have some understanding about what the rules would be.

But in your example, I don't think there is anything there that is inconsistent at all, as you say, with privacy protection.

Senator ROCKEFELLER. Right. Mr. Cate, you indicated in your written statement that you oppose privacy laws. Does that also mean that you oppose laws that protect personal information collected from our children?

Mr. CATE. Senator, I don't believe I did indicate I opposed the privacy laws in my statement. If I gave the impression, it was in error. I certainly support privacy laws and certainly support privacy. I oppose privacy laws that are unnecessarily expensive or don't create a benefit at the same time.

Senator ROCKEFELLER. Now, this is exactly where I want to be, so you need to answer my question.

Mr. CATE. I strongly support privacy laws that protect information collected from children.

Senator ROCKEFELLER. What about medical records?

Mr. CATE. It would depend on the type of record and the context——

Senator ROCKEFELLER. Now, what do you mean, it would depend upon? I mean, you say the word "depend upon," and anybody can go in any direction and nobody will ever know.

Mr. CATE. Senator, that is, in fact, the standard the Supreme Court has long used for evaluating the constitutionality of restrictions on expression is how great is the interest and how closely does the law serve that interest.

Senator ROCKEFELLER. I don't serve on the Supreme Court. I serve on the Commerce Committee. I would like an answer to my question. Do you support medical privacy?

Mr. CATE. I certainly support medical privacy. Yes, sir.

Senator ROCKEFELLER. It depends on what nature.

Mr. CATE. I support privacy. Yes. Absolutely.

Senator ROCKEFELLER. And absolute privacy or privacy absolutely?

Mr. CATE. My support is absolute. I don't believe you can have absolute privacy.

Senator ROCKEFELLER. OK. I will accept that. What about race?

Mr. CATE. Excuse me. I——

Senator ROCKEFELLER. Race, ethnicity.

Mr. CATE. I believe your ethnicity is something that is in many cases reasonably discerned from your appearance, and so, no. I don't believe——

Senator ROCKEFELLER. I am talking about the Internet. I am not talking about face to face conversations.

Mr. CATE. Well, I certainly don't oppose the collection of that information if you disclose it.

Senator ROCKEFELLER. Uh-huh.

Mr. CATE. In fact, Federal law requires the disclosure of that in many instances.

Senator ROCKEFELLER. Now, wouldn't regulations—if you opposed these things or at least several of these things, these regula-

tions would impose a cost on industry, but you accept that cost on industry.

Mr. CATE. I accept that cost if it generates a benefit that exceeds that cost, of course.

Senator ROCKEFELLER. What do you mean by "it creates a benefit"?

Mr. CATE. If the net gain to society from a law is greater than the cost it imposes on society, that would generally indicate to me it is a desirable law.

Senator ROCKEFELLER. Uh-huh. OK. Last year you wrote an article opposing privacy protections. That may have been where I got my first bias from, in terms of my question. It said, "you believe it is wrong for Congress to prohibit states from selling people's home addresses and driver's license information in an effort to prevent stalking or identity theft". Do you believe this still?

Mr. CATE. I believe that it is wrong for Congress to prohibit the states from making available the information that is in the public record unless it is first demonstrated that there is substantial risk of harm from that information being made available. At the time that Congress enacted the Driver's Privacy Protection Act and since then, it has not made that demonstration, and so I believe it was an inappropriate law.

Senator ROCKEFELLER. Would the other two witnesses be willing to comment?

Mr. ROTENBERG. Well, I think contrary to what Fred Cate has said, in recent opinions, the Trans Union versus FTC, and the RISG versus the FTC, the Courts have held that, in fact, a showing has been made by Congress in the area of financial privacy that outweighs the commercial speech interest, so actually I am not quite sure what his point is. I mean, he is correct that there is an analysis under the so-called intermediate level scrutiny view of these types of regulations that requires some demonstration of harm, but the recent decisions, I think, bode well for privacy.

Now, as to the Driver's Privacy Protection Act, he may not be familiar with this. I know Senator Boxer is, because she was involved in the passage of that legislation, but it flowed from a very unfortunate incident involving a young woman in California, and because of that, the state of California and subsequently the Congress passed legislation to place certain restrictions on access to DMV records.

I think even though these points are fairly well established, there is still some risk in saying that we should not have privacy legislation unless we can show that a lot of harm has occurred. A great many people believe to day that they would like to have privacy legislation, so that harm doesn't occur. It would be a good reason to legislate, to avoid the harm that might otherwise take place. But I think the showing as to previous legislation has been established.

Senator ROCKEFELLER. My time is up, Dr. Schwartz. I don't know if——

The CHAIRMAN. Yes. That's all right. Go ahead.

Mr. SCHWARTZ. Very briefly, I supported the Driver's Privacy Protection Act. I think people, when they get a driver's license, expect the state to use that for driving-related information and not

to have it turn into commercial use by private organizations, and I think the Driver's Privacy Protection Act tried to limit the use of such information to only compatible usage.

On the First Amendment issue, I do think there is going to be increased scrutiny of privacy legislations by Courts. I also believe, however, that constitutional privacy legislation can and should be crafted. The cases that we have heard reference to, the Trans Union opinion from the D.C. Circuit and the more recent District Court decision regarding the Individual Reference Services Group, a decision from April 30, 2001, I think indicate how Congress can do it. Namely, they have to carefully identify the particular notion of privacy and the interest to be protected, and then try to craft legislation narrowly to further that interest.

The CHAIRMAN. That is what we have got to do.

Senator ROCKEFELLER. Thank you, gentlemen.

The CHAIRMAN. Thank you.

Senator Allen.

Senator ALLEN. Yes. I would like to ask—each of these folks. I have a lot of questions. At least my microphone works.

As far as the platform for privacy preferences, P3P, it seems to me that that is emerging possibly as an industry standard, and it is an automated way for users to be informed, knowledgeable, and obviously a way of the private sector handling it, and in putting the decisions in the hand of the consumers. Mr. Cate, what is your view of P3P as a development and a way of securing the privacy decisions that all of us share a concern about?

Mr. CATE. Well, Senator, I think it is a terrific development, and I think it is a perfect example of the ways in which technologies may help consumers protect our own privacy, and frankly, do so far more effectively than law can, because it would work outside of just the reach of U.S. law. It would not be concerned with jurisdictional boundaries and things like that.

I think we still have to have some degree of awareness of the fact, for example, that all of our computers today allow us to establish whether we accept cookies or not. However, virtually none of us actually exercise that choice, so the fact that we may now have a technology available, readily available, affordably, in fact, at no additional cost available, that allows us to set our privacy preferences. It will simply be interesting to measure as an empirical matter how many people actually take the trouble to do so and then act consistently with that.

Senator ALLEN. Mr. Cate, let me ask you some more questions here. I have been studying this privacy, various principles and legislation over the years, whether it was the Wyden-Burns bill or Senator McCain's bill or Senator Hollings' bills or Hatch-Leahy, and so forth and so on, Senator Edwards' bill as well.

Do you believe that whatever principles are applied in any legislation should apply to offline as—at least similarly as it does to online?

Mr. CATE. Yes, sir, I do believe that.

Senator ALLEN. Do you have an understanding of the preemption of state laws? What is your view on the preemption of state laws? I know you talked about opt-in and opt-out, but I am trying to get your views on a broader section than opt-in and opt-out.

Mr. CATE. I certainly think Internet commerce, online commerce, is one place where preemption would be appropriate. I am not, you know, generally—I mean, my own legal scholarship does not support preemption as a general matter, but in a place where you have an intrinsically form of interstate commerce and which it is not—Mr. Rotenberg mentioned businesses facing 50 standards. Forget about that. It is consumers facing 50 standards that is the problem, and a single standard that a consumer——

I mean, imagine the complexity. We worry about the Gramm-Leach-Bliley complexity, but imagine if we were getting notices from every single state that were different, instead of the variety of notices that were seen under one Federal law. If there is ever a case for preemption, I believe this is it.

Senator ALLEN. Well, as far as—in the event that there is a violation of those privacy standards, how best would that be enforced?

Mr. CATE. I believe the, if you will, sort of traditional enforcement mechanisms would be either through the Federal Trade Commission or through the states' attorneys general, and that that would seem appropriate in this instance as well, so that states would continue to play a critical role in enforcing these standards but would not play a role in writing these standards.

Senator ALLEN. Implicitly, then, you are saying that you would not prefer or would not suggest a private right of action.

Mr. CATE. I implicitly am saying that and am happy to say so explicitly as well, sir.

Senator ALLEN. And why not?

Mr. CATE. I think there are a number of reasons. One is, frankly, private rights of action tend to not be the best enforcement action, precisely because they become just add-on cases, so that if there is a complaint to the FTC, the FTC launches an investigation, and then we see the emergence of these additional cases, class actions and so forth, and it is unclear what is gained. You know, once the Government has acted or a state attorney general has acted, has brought a case, what the additional benefit is of these other cases.

Also I think the potential damages are quite significant. Again, my good friend Mr. Rotenberg used the example of 500 or $1,000 incident, but if you take an online service provider that has, say, 20 million customers, and you have one single disclosure of information and you multiply it $1,000 times 20 million customers, I think that sort of fairly modest fine could be seen as fairly punitive.

Senator ALLEN. I would like to ask Mr. Rotenberg and Mr. Schwartz to comment on the impact, to the extent that they can, on United States companies due to the European Union's privacy directive, what impact that has had on consumers, but mostly to U.S. companies in Europe, if either of you could comment on that.

Mr. ROTENBERG. Senator, I can't speak for U.S. companies, but I can say this, that as a result of the EU directive and the safe harbor arrangement that was negotiated between the United States and Europe, European consumers have now at least a bit of confidence that when they do commerce with U.S. firms, they will get the type of privacy protection that has been traditionally associated with European privacy law. It has, in effect, raised the standard of practice for U.S. firms, allowed further entry into European mar-

kets, and opened up new commercial opportunities, and I think this is or should be good news. I mean, this is the way the privacy laws should operate.

The goal is not to restrict business activity. The goal is to promote consumer confidence and enable firms to conduct business in a way where privacy is protected, and I think the EU data directive and the safe harbor arrangement have furthered that goal.

Senator ALLEN. Mr. Schwartz.

Mr. SCHWARTZ. As I testified, I am very encouraged by the important information age companies that are signing up for the safe harbor. The EU directive has been a long time coming. It was enacted in 1995. It took effect in 1998. European countries are now harmonizing their legislation to reflect its high standards, and now we have the safe harbor arrangement. I think we can hope, at least, that it is going to have a positive impact on American companies. The hope is that American companies will provide the same level of protection to the personal information of American citizens that they do to the transfers of information from Europe that they are pledged to protect under the safe harbor.

Senator ALLEN. Thank you. Thank you, Mr. Chairman.

The CHAIRMAN. Very good.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Gentlemen, last week Eli Lilly blamed a programming error for a problem where they accidentally disclosed email addresses of about 600 medical patients. My question to you is: Do you all believe—we can just go right down the row, start with you, Mr. Rotenberg—that with a sensible privacy policy in this country, that those kinds of problems and ones that could conceivably far more serious would be less likely?

Mr. ROTENBERG. Yes, Senator. I think a good privacy policy, backed up with enforcement, would make those incidences less likely.

Senator WYDEN. Mr. Cate.

Mr. CATE. No, Senator, I do not. In fact, I would note that information was collected pursuant to an opt-in requirement.

Senator WYDEN. Mr. Schwartz.

Mr. SCHWARTZ. I think that we have incidences of what has been called the "revenge effects" of technology. In the information age, it is very, very difficult to avoid the consequences of the kinds of networks that we see, so I don't think privacy policies will make that go away. What we need is ongoing vigilance against these so-called "revenge effects," as we have more and more use of technology in our lives.

Senator WYDEN. Mr. Rotenberg, I think one of the key questions is whether we are going to have one standard or 50. I touched on it; so did you. I am curious whether you think that preemption, something that would ensure one standard, is inherently bad. In other words, if the U.S. Senate set the bar in the right place and did it in a fashion so as to ensure sufficient flexibility to promote the innovation that you are talking about, what would you be concerned about if the Congress went about it that way?

Mr. ROTENBERG. Well, Senator, as I said in my statement, my concern really flows from studying the history of privacy law in the

United States and seeing the Federal baseline enabling states to innovate and respecting our Federal form of government. I think those traditions are important ones, because states, in given that freedom, oftentimes will come up with better solutions. We have seen this.

I mean, 10, 12 years ago, there was a lot of discussion about Caller ID, for example, and it was the state regulatory authorities that took the initiative there and led to the development of stronger privacy protection for telephone customers. Today there is a big debate taking place about the privacy of genetic information, and this is another area where Congress has focused attention, but it has been the states that are leading.

So I appreciate your point. I think if there were, as you said in your statement, meaningful privacy protection with preemption, that would certainly be better than a weak statute. But even meaningful privacy protection, I think, would lose an opportunity that history suggests we should try to preserve.

Senator WYDEN. Well, I want it understood that as we work on this issue, I want to make sure we don't close off the opportunity for that state innovation that you are talking about. I mean, with the Electronic Signatures Bill, for example, we worked very hard to ensure that there was a role for the Federal Government, and there was a role for the states, and I would just hope that we could figure out a way at the end of the day to have one standard rather than 50 and do it so as to encourage the innovation you are talking about.

Last question I wanted to ask each of you is: Is it the case that there are people today in the private sector who are doing the job right? Is there a company, more than one company, a set of organizations, that we can look to that really sets the bar in the right place? Why don't we start with you, Mr. Schwartz, and just kind of go down the——

Mr. SCHWARTZ. Sure. I think one interesting development has been marketing companies who are shifting to opt-in because of their belief that they will get higher quality information from consumers that they will be able to sell at a higher price. The difficulty from the consumers' viewpoint is—and this gets back to my point about the failure in the privacy market—it is hard to keep your information from being collected from the other companies. So you are kind of stuck there. You would rather do business with the good opt-in companies, but you are stuck with the Hobson's choice of doing business with everyone.

Another, I think, positive development is P3P. However, I don't think technological solutions will be a silver bullet. I think you run into a chicken and the egg problem, where unless a lot of consumers decide they want to use P3P, and unless a lot of companies enable their sites to be P3P enabled, it may never take off.

Senator WYDEN. That would be your answer to the question, that P3P is in line with where you think we ought to be going in this country.

Mr. SCHWARTZ. My solution is that I think that both opt-in companies and P3P are part of the solution, but I don't they are going to get us everywhere where we want to get without privacy legislation.

Senator WYDEN. OK. Mr. Cate.

Mr. CATE. Senator, I don't know that we necessarily see any perfect solutions in the market, and I feel like I should also note in many instances privacy being a very personal concept, privacy is in the eyes of the beholder. I was interested to see that *USA Today* on Monday cited American Express's privacy policy as one that it disliked the most. Three weeks ago in California, the chairman of the banking and finance Committee there in the assembly cited American Express as the finest example of a privacy policy that had been mailed out and had it distributed to every person in the audience in the hearing room, so that they could copy that example. So it is a little hard to figure out sort of what is best.

But I would say, I think many online companies have done a very good job in being clear about what they do with information, about making clear about what consumers' rights and opportunities are, and in really building consumer support and confidence. That is really the name of the game.

Senator WYDEN. Mr. Rotenberg.

Mr. ROTENBERG. Senator, we have had a simple measure for this question from the start. The question we ask is simply this: Are companies fully applying and enforcing fair information practices? That is the standard for us. On the technology, we think——

Senator WYDEN. But is there a company out there—you are one of this country's premier privacy authorities, and your view counts a lot with me. Is there a company or an organization in your view that is doing the job right today?

Mr. ROTENBERG. Senator, in my view, there are many companies that are doing a good job addressing privacy issues, but frankly part of trying to maintain our role in the privacy debate has required also that we keep some distance from these companies. We don't consult for them. We don't advise, and we don't endorse. We are interested solely in promoting the very best privacy protections for American consumers, and we will recognize when companies do a good job. But I would be very reluctant to name a company this morning.

Senator WYDEN. My time has expired, but be assured that I am going to ask you this question privately, because I value your view. Nobody is talking about endorsing a product. What we would like to know is whether there are some people out there that are doing the job right, so it can help us as we try to fashion legislation.

I thank you, Mr. Chairman.

The CHAIRMAN. Very good. Senator Stevens passes, so Senator Boxer.

Senator BOXER. Thank you, Mr. Chairman.

This is one of the most fascinating issues, because I think that it is simplistic to say there is an anti-business or a pro-business view, regardless of how you view this. My view is that when you look at the polling, it says 79 percent of those who did not buy gifts online in the 2000 holiday season said they did not like to send credit card or other personal information over the Internet. So some people aren't going online, because they are a little afraid that their information will be sold.

Also, concern about privacy is the single most cited reason Internet users give for not making purchases and for non-net users de-

clining to even go on the Internet. So I think if we do come up with something that is a smart, good, balanced plan here, I think we will, in fact, be helping consumers and business. That is why I work with John Kerry and Senator McCain, because I felt we did so try to come up with that balance.

I wrote the Driver's Privacy Protection Act, and it was, in fact, the State of South Carolina, Mr. Chairman, that questioned that Driver's Privacy Protection Act. They wanted to sell people's licenses, and they appealed the constitutionality of this particular law all the way to the Supreme Court, and I was in the audience when the Court heard the case. It was a 9–0 decision, upholding the Driver's Privacy Protection Act, and I think it is because of the nature of what was happening with these lists.

They were being sold without people's permission, and as Mr. Rotenberg said, it was a very tragic case that led me to write this particular law, because people were stalking other people, finding out who belonged to what license. So having said that, you would think that I am for the most—the strictest kind of privacy on the Internet. But I think what we are coming up with here is the fact that there isn't a one—this is my view—a one-size-fits-all kind of deal.

Having seen the Eli Lilly horrible situation, which Mr. Cate said, "Well, people opted in", they didn't opt-in to have the fact that they are taking a certain drug put out on the Internet with their email address. They opted in to be reminded about taking the medicine, so there was a misuse here.

So, I guess, Mr. Cate, I want to ask you this, and you kind of answered it, but I want to get it on the record in a clearer way. Do you think that as we try to work together—and I really think there is a desire for us to do that—on a national privacy act regarding the Internet—because you are right; if you have 50 different laws, it is a nightmare. If you have this kind of law, do you think we could put our heads together and come up with opt-in and opt-out combinations, because frankly if I buy cookies online, I think opting out is saying, "Look, I opt-out. Something pops up on the screen; don't sell my name to other cookie people". You know, that is OK, and if somebody makes a mistake, and I get something about cookies, it is no big deal. But if I am taking a certain medicine, and I want to retain my privacy, that is a whole other deal.

So do you think—do you see that as that we could, in fact, fashion something without being too specific, because I don't think that is the way we should do it. Is there a way that we can have broad categories for opt-in and opt-out?

Mr. CATE. Yes, Senator. I think that is absolutely correct.

Senator BOXER. And may I ask the other gentlemen if they could see that there is a—did you want to add something to that or——

Mr. CATE. I always want to add something, but I will stop there in deference to my colleagues.

Senator BOXER. Mr. Schwartz, Mr. Rotenberg, can you see that as a possible way for us to go?

Mr. SCHWARTZ. Yes. I absolutely think that a mixture of both opt-in and opt-out rules, as I said before, would be the way to take care of this at the least cost to consumers. I also think, to follow up on your point, that there is a tradition of privacy legislation

helping industry. An example would be the Fair Credit Reporting Act which I think contributed to the explosion in credit card use because of the consumer confidence about that information.

I recently saw that cell phone manufacturers and cell phone companies are calling for legislation about wireless location dates, because they think that cell phone use will stagnate unless there are limitations on how that information is used. So I think pro-privacy legislation can also help industry.

Senator BOXER. And, of course, the Fair Credit Reporting Act does apply to the Internet, so that is good.

Mr. Rotenberg, this idea of us working together on a combination of opt-in, opt-out?

Mr. ROTENBERG. Well, Senator, I have a somewhat different view of this issue than my colleagues. I think you need both opt-in and opt-out; I think they go together. But the relationship is a little bit different than the one described by Mr. Cate and Mr. Schwartz. I think you need opt-in at the front end to obtain real and meaningful consent, so that everyone understand what they are getting themselves into, and I think you need the right to opt-out on an ongoing basis if you decide that you are no longer satisfied with the relationship. I think it is the nature of all commercial transactions that common-sensically, we understand the exchange of things for value in this fashion.

Now, I appreciate it is convenient to say, "Well, maybe if it is less sensitive information, opt-out would work, and for more sensitive information, opt-in might work", and certainly bills have been done on that basis. I am aware of it. But I do believe that over time, the better approach, particularly because there is difficulty always in drawing that line, is to say, "Let's have explicit opt-in at the front end; let's obtain meaningful consent, and let's retain a right to opt out if someone isn't happy".

Senator BOXER. Well, I agree with the two-to-one decision of the panel. Thank you.

The CHAIRMAN. Thank you very much.

Senator Nelson.

Senator NELSON. Mr. Chairman, I did not make an opening statement, only to express my gratitude for the opportunity of being part of this Committee, and——

The CHAIRMAN. We will include your statement in the record if you want.

Senator NELSON. Well, I am going to make it right now if——

The CHAIRMAN. Make yourself at home.

Senator NELSON. I want to start out by saying that I, too, as Jay Rockefeller, would be outraged if there was a history of my transactions available to the public such as this. I come to this discussion today with some interest and some background in this area, for a Supreme Court decision back in the mid-90s entitled, *Barnett Bank* v. *Bill Nelson,* in my capacity as insurance commissioner, decided on a technical reason, that heretofore banks and insurance companies could merge, and I knew as insurance commissioner that there was the threat of the loss of privacy, that after Gramm-Leach-Bliley, we have seen exactly that.

We have seen in the merger of banks and insurance companies that a person's personally identifiable medical information, because

they had a physical exam in order to get a life insurance policy, and the life insurance policy now being a part of a bank holding company, that that information can be shared within that holding company. Even worse, that information can be shared outside of that holding company by contracting in a marketing agreement with a third party.

And so when it comes to the issue of privacy on today's discussion on the Internet, I approach this with the view that there are certain things that are inviolate to keep us from moving to the age of Big Brother, that clearly we ought to have, and in my judgment it would be for personally identifiable medical information.

As the Senator from Oregon had just pointed out with Eli Lilly, in this particular case they are saying it is a mistake, but let me tell you what the mistake was. It was 600 people on Prozac, now information totally available to the world, on very personally identifiable medical information. So when it comes to the question of whether or not you should share this privacy, I think it ought to be with the express written consent on medical information.

On personally identifiable financial information, in the merger of banks and insurance companies, I think using the term of art here, opt-in, which is express consent, that clearly it ought to be. And so I come to this discussion intrigued that there really ought to be a basis of common sense that would govern us here.

For example, when we get on in the Internet to interactive television, what is going to be the privacy on that? Shouldn't we be having the right of privacy on an interactive television conversation over the Internet?

So, Mr. Chairman, I will defer from asking any questions and look forward to learning a lot, but that is clearly the background that I bring to the table. And I am absolutely fascinated in this. I filed the legislation to correct what I consider the promises that were made in 1999 in the enactment of the Financial Services Modernization Act, otherwise Gramm-Leach-Bliley, of which that huge gaping hole on not protecting privacy has not been filled when, in fact, it was promised. And I look forward to working with you, Mr. Chairman, on this.

The CHAIRMAN. You are one of the best witnesses we have had.

[Laughter.]

The CHAIRMAN. I will include in the record Monday's editorial in *USA Today* that verifies just exactly your idea about Gramm-Bliley, Confusing Privacy Notices Leave Consumers Exposed. We will include that in the record.

[The information referred to follows:]

[From *USA Today,* July 9, 2001]

CONFUSING PRIVACY NOTICES LEAVE CONSUMERS EXPOSED

(Our view: Millions of records open up as people fail to 'opt out.')

FINANCIAL PRIVACY

Imagine spreading out all of your most personal financial data on the kitchen table, then having hordes of strangers storm in to browse, copy, share it with business partners and sell it to telemarketers. You could keep your privacy only by following detailed, legalistic instructions each time a new snooper tries to barge through the door.

Millions of bank customers and credit card holders are in this situation this week, only the instructions are so confusing, many unwittingly threw them away.

Welcome to the system Congress set up in 1999 to protect financial privacy. Banks, credit card companies and others who know how you spend your money can share and sell that information unless you explicitly "opt out."

Because fewer opt-outs mean more profit, the results are no surprise. When a July 1 deadline rolled around for giving customers their choice, the financial institutions made the notices as confusing as possible.

Just look at some of the notices consumers have received:

• One sent by American Express is written at the graduate-school level, according to a report for consumer advocates by readability expert Mark Hochhauser. Little help to the 92% of adults with less education.

• Wells Fargo Bank sent out a notice that is 10 pages long, with no phone number to call to opt out. Consumers must fill out a form, detach it and mail it at their own expense. A Wells Fargo spokesman says it didn't want to "overload" its phone system.

• The notice from Chevron Credit Bank offers a toll-free number, but it's open only weekdays 7:30 a.m.–4:30 p.m. PT. But to apply for a credit card? That number's available until 11 p.m. weekdays and until 5:30 p.m. Saturdays.

Little wonder, then, that despite widespread public concern about financial privacy, fewer than 1% of consumers had exercised their right to opt out by mid-June, the American Bankers Association (ABA) estimates. An ABA survey in May found 41% could not even recall receiving a notice.

The bankers trade group offers transparent excuses, saying institutions merely followed model notices put together by regulators. But nothing in the regulations prevents a bank from adding plain English on top of the legalistic jargon. Something like: "If you don't want us to share your personal data with telemarketers, here's what you can do."

Congress caved in to the opt-out system pushed by the financial-services industry, which showered politicians and their parties with nearly $200 million in the decade before the bill was passed.

Had Congress listened to consumer groups and privacy advocates instead of its campaign contributors, it would have instead created a far more protective "opt in" rule. That would have required banks to get customers to say yes before any information could be shared.

You can bet that if bankers had to go begging for consumer permission to sell this private data, the notices would be plenty clear and quite memorable.

It's not too late to tell banks they can't dispense your financial history at will. Customers can say no at any time.

But if lawmakers want to protect consumer privacy in the future, they need to make would-be snoopers ring the doorbell first.

The CHAIRMAN. Senator Edwards.

STATEMENT OF HON. JOHN EDWARDS, U.S. SENATOR FROM NORTH CAROLINA

Senator EDWARDS. Thank you, Mr. Chairman. Am I allowed to ask Senator Nelson questions?

[Laughter.]

Senator EDWARDS. Well, first of all, I want to thank the Chairman for his leadership in this area. He has been a real force for protecting people's individual privacy, and we appreciate all the work the Chairman has done in this area.

I start with a very simple idea, which is that people ought to have control over their own personal private information, and married with that a practical idea which is when I think, for example, in the context of financial services—and I was involved in that legislation—when you mail somebody something, whether you have an opt-in or opt-out policy, as a practical matter, 90-plus percent of people pay little or no attention to it. And so I think you essentially decide the result when you choose either opt-in or opt-out, if they are the exclusive remedy.

What I would like to talk about is what I think I heard Mr. Schwartz mention a few minutes ago, which is maybe a more creative solution to this dilemma, something that would allow us to put together some of the technology innovations that have been done by people like Microsoft with P3P and legislation, because it seems to me there ought to be some way to marry these concepts, opt-in, opt-out, and the use of technology, in a way that is effective, that allows people to really maintain control over their information, but at the same time, doesn't hinder the use of the Internet.

Now, I don't know what that solution is, but if we get away from just the academic conceptual idea of the only choice, the Hobson's choice in this case, is between opt-in or opt-out and ignores the use of technology, it seems to me that those things ought to work together in combination in some fashion, and I would just like to hear a comment from each of you on that subject.

Mr. ROTENBERG. Well, Senator, we have been thinking about that issue for a long time, and we have been doing so in part because we think that to effectively protect privacy, legislation will not be enough. I mean, I am happy to be here today and explain the need for legislation, but I think we also need very good technology. Our organization EPIC was at the forefront of the battle to reform encryption policy, because we saw the need to make strong tools for online privacy available, and we continue to promote the availability of good technology for privacy.

But I have to say this, Senator, and I know again I am probably going to be in the minority side of a two-to-one opinion. I do not believe that P3P as currently conceived is going to promote online privacy, because it lacks the essential elements of privacy protection, of setting the bar high enough to limit the collection and use of personal information to afford any real safeguards.

Senator EDWARDS. Can I interrupt you just a minute?

Mr. ROTENBERG. Yes.

Senator EDWARDS. I understand that, and I understand there are concerns with that particular technology. But my question is more conceptual. Is there not a way to——

Mr. ROTENBERG. Yes.

Senator EDWARDS [continuing]. Use technology in combination with legislation?

Mr. ROTENBERG. The key, I believe, to privacy solutions using technology is to minimize the collection of personally identifiable information. You see, it is the collection of the data about you, your address, the members of your family, your financial circumstances, all of this that gives rise to the privacy problem.

I mean, if we were talking about the environment, we would basically be talking about a form of pollution. It is sort of the byproduct of production. If we can find a way to limit the generation of that personal information and still enable online commerce and still enable people to receive and exchange information, I think we will go a very long way by technical means to protecting privacy online.

It is the reason, for example, that people who study Internet privacy feel so passionately about anonymity. Now, to a lot of us, you may think, Well, I am little bit concerned about people who want to be anonymous. But if you think about it for a moment, most

transactions, cash-based transactions, most activities, walking down a street, reading a book, going into a movie theater, these are all essentially anonymous transactions.

And so we see the bedrock for online privacy in the technological realm as trying to preserve anonymity, and from that, a lot of things, I believe, will be possible, and I think it coexists very nicely, in fact, with legislation, because legislation says, "And at the point that you start to collect personally identifiable information, then we are going to impose some legal burdens on you, but if you can do what you want to do without collecting data——

Senator EDWARDS. But shouldn't people have the personal privilege or right to decide they don't mind if their personal information is being collected?

Mr. ROTENBERG. Absolutely. I mean, we do not argue against the right that everyone has to disclose information, to go on a television talk show, to do whatever they wish to publicize their private life. That is a choice that every person always has. The question is: Do they have the right, even in the most public of careers, to then spend time with their family, to then pick up a telephone, to then have a private conversation with a colleague, and not have that information disclosed to others?

And for that to happen in the online environment, I think we are going to need very strong techniques.

Senator EDWARDS. Thank you, Mr. Rotenberg. Mr. Cate and Mr. Schwartz, I want an answer, but please make it very brief, because I have got one other subject I want to cover very clearly.

Mr. CATE. Yes, Senator, I agree. I think you put your finger right on the point, which is that the goal of privacy law should be to empower consumers, to put as many tools as possible into our hands, and technology is clearly one of those critical tools.

Senator EDWARDS. Mr. Schwartz.

Mr. SCHWARTZ. I think that good legislation can stimulate their use of the right kind of technology. I think as a model for that, the Child's Online Privacy Protection Act allows industry to draft safe harbor standards as to how to get parents' consent at the least cost to parents. Those safe harbor standards are scrutinized by the FTC, and the FTC has to approve them. This legislation didn't try to micro-manage the way industry could go about getting parental consent, but let industry figure out how to do it at the cheapest cost using technology.

Senator EDWARDS. Thank you. I want to continue to work with you on this issue, because I think there is a way to do this. Second, I want to change the subject briefly and talk about something called location privacy, which is—this whole privacy issue fascinates me, but location privacy has been something I have been thinking about a lot recently.

You know, everyone in this room who has a cell phone, a pager, a Palm Pilot, somebody, some company somewhere knows where they are, and people who use these OnStar directional systems in their cars, which are becoming more and more prevalent, also people are going to know where they are in their automobiles.

And it seems to me that that—and I think there is some recognition of this—that is information that is private, and people may want to maintain some control about. I am introducing legislation

today, in fact, on this subject, to provide people control over that information and specifically to require their permission in order for whatever company has that information to give it to—sell it or use it, give it to third parties.

But I am interested in each of your perspectives on that issue, whether you think it is important to protect people's personal information about where they are located, particularly when they don't want that information disclosed, but the only reason somebody else has it is because they are using a cell phone or they are using a pager, or they are using one of these new systems.

I might add that we have been working with the people involved in all of those industries, and I think they are concerned about the same thing. I think they care about their customers' privacy, so they have been working very closely with us on this, but I am interested in your comments about that, starting with you, Mr. Rotenberg.

Mr. ROTENBERG. Senator, I think this is one area where establishing privacy protection at the front end could help establish consumer confidence in the offering of these new services and give people the assurance that when they take advantage of some of these new services, their privacy will be protected. I really wonder at this point, with the recent experience of the Internet, if the cellular industry wants to go through the whole self-regulatory exercise again with everything that came about from that.

Senator EDWARDS. If I could interrupt you just a minute, one of our goals in this is to try to deal with this on the front end, so that is one of the things we hope to accomplish.

Mr. ROTENBERG. Right. I mean, some of the practical problems that have been identified, for example, is how do you provide a privacy notice on a cell phone screen? It is just—it is not going to work. I think my colleague, Mr. Cate, even acknowledged recently that this seemed to be an area where legislation was appropriate. And I think here again, good privacy legislation will be good for consumers; it will protect their data. It will be good for business, because they will be able to provide some assurance to their customers that their information won't be misused.

Senator EDWARDS. Mr. Cate and Mr. Schwartz, my time is up. Just give me a couple sentences each, please.

Mr. CATE. I agree. I think it is a critical issue. I think in reality it is going to be a tremendously vexing issue, because it shows the difficulty of this sort of dialog of notice and choice and all of this, because there is, as Mr. Rotenberg says, "really very little room in that for a screen".

And finally it highlights the fact that, I think, frankly what most people in the cases we have seen so far are worried about is Government coming and subpoenaing those records, and no amount of privacy policy is going to deal with that, because you can't insert a contract to protect you from a Federal action.

Senator EDWARDS. Mr. Schwartz.

Mr. SCHWARTZ. I just want to comment on one thing which is a knowledge gap in this area. It is not only that we have to worry about cookies and web bugs, but here we have another area in which there is likely to be an information asymmetry between the people who collect the information and the consumers. I think leg-

islation could help that, because you are not going to have a negotiation when there is that gap in knowledge.

Senator EDWARDS. I thank the witnesses very much, and I thank the Chairman for his indulgence.

The CHAIRMAN. Thank you.

Senator Kerry.

STATEMENT OF HON. JOHN F. KERRY,
U.S. SENATOR FROM MASSACHUSETTS

Senator KERRY. Thank you, Mr. Chairman.

Let me begin, if I may, by just saying to my colleagues that I am circulating a letter and ultimately will be putting in a resolution on P3P, urging all of us in the Senate to make our web sites P3P compliant, and ultimately that we should be urging all government entities to do so. The chicken and egg issue that was raised earlier is a real issue. You won't have the software developed and available unless people are making machine-readable capacity at their sites and vice versa, so it goes together, and I think we need to set the example and try to move on that.

Second, with respect to the issue raised by Senator Boxer and Senator Edwards, I have talked to Senator Hollings, our Chairman, about this. Senator McCain and I will be reintroducing our legislation, but with some added detail this time. I think the mistake we made before and I think the mistake we are all making here in this discussion is that this is being made somewhat more complicated than it needs to be, and that is because we are confusing medical and financial requirements and demands with privacy with a pure commercial transactional demand, and there are distinctions.

There are distinctions, obviously, in the Supreme Court in terms of commercial speech, and there are distinctions in the weights that we have heard discussed here about what sort of public interest is measured against the restraint that we put in place to support that interest. And in the balance—and I have talked to the Chairman about this privately—I believe there is a mix and match here, that there is a much easier way to have opt-in, where opt-in is appropriate, almost obviously, as a matter of common sense, on medical information and financial information, but that precisely because of the delicate nature of the commercial transaction and the status of the Internet and all of the interest we have in its future development and the potential for sales, et cetera, and the need to still fulfill the full measure the experiment here about whether or not you can survive on advertising or not or how it is going to work, there is a marketing component where there is just no harm, where you can't measure harm, and we shouldn't be getting so excited about it.

The mistake, I think, that Senator McCain and I made was we were silent on the issue of medical and financial, because they were being sort of dealt with out there in the other universe, and I don't think you can be. I think it is too easy for people to say, "Well, wait a minute; how are you going to deal with this particular component". It is absolutely clear, Mr. Chairman, that financial information deserves the most privacy you can give it, and there ought to be sufficient protection. Likewise, medical, absolutely. What we have heard described here is unacceptable by any standard.

But—and, again, here is where we are all missing something—the debate is really not so much centered on opt-in versus opt-out if you have adequately adhered to the five principles that have been set out by the FTC and by most observers with respect to notice, adequate notice; adequate choice; adequate access; adequate security; and adequate enforcement. If you have each of those sufficiently, then opt-in/opt-out becomes a much more diminished sort of argument. And I see you are nodding your head, Professor Schwartz, and I think you would agree that there is sort of a confusion here.

Now, if—let me ask you each sort of a fundamental question here. Are we concerned—should this Committee be concerned with a generic American citizen right to privacy, or are we concerned with some specialized thing called privacy on the Internet?

Professor Schwartz.

Mr. SCHWARTZ. There are two trends here that are colliding. One is the trend of convergence. The Internet is now being incorporated into more aspects of our life, so we may be accessing it through a telephone or a television. It becomes increasingly difficult then to view the Internet as an abstraction. The difficulty, however—and I don't have a solution to this—is that the American tradition of privacy legislation has been sectoral in focus. So to that extent it is quite appropriate to be looking at privacy legislation for the Internet. That has traditionally been the way that we have done it, but there is this tension——

Senator KERRY. Well, I don't disagree. I don't disagree at all, but I think each of you—Mr. Rotenberg, you and I have discussed this in previous hearings. We have kind of been over this ground before, and I think we are talking past each other a little bit. If privacy is the concern of Americans—and Senator raised this earlier a little bit—you have a right to privacy in Stop-and-Shop or Safeway or any store, just as you do on the Internet.

If the information when you walk into a department store is used to market to you, do you deserve the same protection for that as you do for the marketing, for the browsing that you do within the Internet, if the only harm is the potential that you are going to receive a solicitation? So is the protection the same?

Mr. SCHWARTZ. I think the concern for privacy, yes, is the same, and the focus of legislation, to the extent that you want to have legislation, should be at the moment of collection to the extent you see that there is harm.

Senator KERRY. But you see—and I think each of you would agree with this—if we—we wind up picking winners and losers. If we are only focused on the Internet transaction, we create a requirement that applies to a sale in one place but doesn't apply to a sale in another place. Where is the equity in that, Mr. Rotenberg?

Mr. ROTENBERG. Well, Senator, I understand your point, and I don't think it is appropriate to impose different rules, but at the same time——

Senator KERRY. But we are being asked to.

Mr. ROTENBERG. Not exactly, sir. You see, the Internet by its nature, because it is an interactive digital environment, creates privacy risks that simply do not exist in the physical world. If you go into a supermarket, the only cookies you are going to find are on

aisle 7, and they are going to have a blue bag around them. But if you go onto the Internet, every web site that you go to potentially is going to try to place a tracking technique on your computer. There is——

Senator KERRY. I agree with that. I completely agree with that, but that then depends—you see, but the question is still the same. Does the same right of privacy attach to the potential of a solicitation that comes out of the tracking of your purchases over a period of time at a store versus the tracking that takes place of your browsing or journeys on the Internet? That's question No. 1.

And No. 2: If we were to adequately do the mix and match that we have talked about, so that you have the adequate notice, the adequate security, the adequate enforcement, the adequate choice, and you are opting into that or opting out, as the choice may be according to what the potential harm is, you can provide the protection for the financial, provide the protection for the medical, prohibit the cookies, maybe even make an opt-in where cookies are involved, make an opt-in where you have the lack—where you have any other kind of tracking for your journeys as a whole, but not interfere necessarily with the more mundane, normal, transactional, routine effort that people are more concerned about.

And that is where, I think, you find the most concern in terms of whether or not it is a choice of opt-in/opt-out ultimately. It seems to me you can provide the adequate protection and provide for a range of technological fixes simultaneously. Would you like to comment?

Mr. CATE. Yes, Senator, I would. I think that is exactly correct. In other words, when you said earlier focus on the harm, where is the harm, that that is exactly the point. If Congress were to deal with the issues where there is a real threat of harm or sensitive financial or sensitive medical information, as you have already dealt with the situation of children, much of this issue would presumably go away.

The problem has been that many of these laws being interpreted much more broadly, so, for example, Gramm-Leach-Bliley, which I think everybody would support some level of privacy protection for financial information, but in the hands of Federal regulators, financial information got defined to include your ZIP code; it got defined to include your address; it got defined to include things that most of us don't mean when we mean financial information.

We already see from HHS the same movement in health information, where in order to have health information de-identified, it has to be de-identified, for example, to the year of treatment. Well, I just don't think the month I was treated is highly sensitive medical information, as I was trying to intimate earlier in the dialog with Senator Rockefeller, so it depends on how you define these.

But if you define them so you deal with information that poses real risks, that is precisely where a legislative solution is desperately needed.

Senator KERRY. All right. Fair enough.

Well, I think, Mr. Chairman, that is precisely what our bill will set out to do this time, and I certainly want to work with you to see if we couldn't make that mix and match adequately, but what we are going to do is not be silent this time. I think we are going

to be more specific, more comprehensive in that regard, and it seems that if you have adequate notice, choice, access, security and enforcement, and then measure the act of sort of opening up your site and deciding where you want to go, that is a form of opt-in in and of itself.

I mean, the minute you turn on your computer and sit down at it, you are opting in, and the key here is to know where you are going in terms of the cookies and the other intrusions that people are not necessarily aware of today.

Thank you, Mr. Chairman.

The CHAIRMAN. I won't be silent either.

Senator Cleland.

STATEMENT OF HON. MAX CLELAND,
U.S. SENATOR FROM GEORGIA

Senator CLELAND. Thank you very much, Mr. Chairman. I opted in to coming to the hearing, but after seeing the complexity, I am about to opt out.

I am—I guess my mind seeks to make some sense of all this by trying to search for the fundamental issue here. We talked in terms of privacy, and of course, the American people want private transactions, whether it is on the telephone, whether it is watching television, whether it is on the Internet, or whether it is shopping. I wonder if the ultimate issue is not so much privacy or even secure telecommunications or even interactive communications, but in terms of what we are after here, a comfort level by the consumer without which the commerce does not move forward.

I mean, after seeing the printout of what Jay Rockefeller catches on his Internet, I am kind of glad I don't have a computer at home. I don't have a television, so I am being more disconnected, not so much for fear of invasion of privacy but hearing what I hear about how people can track me if I had a computer and access to Internet, that gives me pause as a citizen, and our citizens out there have great concern about this.

I wonder if the ultimate question is about who chooses what, not so much what they choose, opt-in, opt-out, but who chooses. Who is empowered here and who is disempowered? I mean, it seems like the whole great blessing of the Internet can also be a curse. We can sow to the wind, and we can reap the whirlwind. We have sown to the wind, and it is a blessing in the sense that we are more connected. We know more about each other than we ever thought we would ever know, and a lot of that is good; a lot of that is healthy.

But I think people basically want the power themselves to determine when anybody knows anything about them. It is one thing to turn on a TV, a one-way interaction here, and watch it while sitting in the privacy of my home. It is another thing to turn on a television in the privacy of my home and realize everybody is watching me. That is a whole new dimension here, and as we get into interactive television and other forms of interactive communication, where I am, what I am watching, what I am doing and how I am communicating will be more and more broadly known.

So I think therein is the challenge here: how to continue to lower the barriers that have been there for communications, how to open up communications, whether it is e-commerce or personal commu-

nications, but then how to retain the power of the individual to be empowered to determine when other people see me, see what I am doing, and have access to me and my information.

I mean, it seems to me that that might be the crux of the matter. I get lost in the opt-in/opt-out, although I identify with Mr. Rotenberg here that maybe we talk about a blend here. But how knows where to draw the line, and is it really possible to draw that line in legislation? I mean, I don't think I am quite smart enough to. I mean, I do see where the European Union has tried to do it and where some 70 companies have signed up with the EU privacy safe harbor concept, including Microsoft.

The safe harbor requires notice, opt-in for sensitive personal information, opt-out for commercial marketing personal information, and a right of reasonable access and security. Safe harbor also prohibits the onward transfer of personal information to third parties unless those parties also adhere to the safe harbor concept. So, I mean, that is the European Union. They have moved on it, and some 70 companies have signed up. That is one way to go about it, to increase the sense of security about what people are communicating about.

But I wonder if the real answer isn't this whole question of who determines whether or not I am looked at, whether or not I am tracked. Mr. Rotenberg, do you want to comment?

Mr. ROTENBERG. Well, Senator, I was going to say that I actually thought your point really goes to the heart of the issue, perhaps more so than the debate over opt-in and opt-out and preemption or private right of action, all those other specific provisions. What privacy laws seek to do is to give people the ability to control the use of their personal information, to enable people to do business with their banks and to give sensitive information to doctors and a whole host of other things.

But at their core, the intent is to address the concern that you identified: How do we control this information about us? And I think the reason that we need to stay focused on that issue as opposed to some of these other line-drawing issues is that first of all, those line-drawing issues are very difficult, and second, they can be misleading. It is tempting to say, for example, that medical information, financial information, is particularly sensitive, so that we will give a high standard to, and we will do something else with the rest of the information.

But what do you do when you find out, for example, that rental car companies now have the ability to track you when you are driving your car, and they know, for example, when you drive too fast? Millions of Americans learned this past week that that was taking place, and they were very upset about it. It didn't fall neatly into the bin marked, Medical information, or the bin marked, Financial information, but it was, I think, very much a part of what you were describing. It is the ability to control information about oneself.

Senator CLELAND. If they ever find out what we are doing on a Saturday night date in the car, then we will all be in trouble.

Mr. Cate.

Mr. CATE. Senator, I think you are exactly right. The question is, you know, who makes the decision and on how much knowledge—you know, what knowledge or information do they have

when they make it? I think when you think in the context of the Internet, we have talked a lot about the ability of the Internet to be a privacy compromising technology. It is also a privacy-protecting technology. It offers the ability to appear to the world without appearing physically, the ability to block a fair amount of information about oneself.

The list that has been circulated of Mr. Rockefeller's browsing habits, which I have not seen but would love to, Senator is taken from his computer, the computer obtained in his office, just like if a checkbook were in the office or if a credit card statement were in the office. And interestingly, the technology is there to block the recording of cookies, to clear out the cache so that there is no record of where the computer has been; in other words, to put the individual entirely in the driver's seat.

But even the failure to exercise that means only that if somebody breaks in your office or is authorized to come in and look for that information, they find it. And there is a question of how much farther should law go to protect us.

Senator CLELAND. Mr. Schwartz.

Mr. SCHWARTZ. I think the point about trying to empower and shifting power to consumers is a critical one in this debate, and I also agree with you regarding this issue about the comfort level for consumers, which we have discussed today, and about how good privacy legislation will hopefully stimulate e-commerce and increase this comfort level.

Senator CLELAND. Thank you all very much. My time is up, Mr. Chairman. Thank you.

The CHAIRMAN. Very good.

Senator Ensign.

STATEMENT OF HON. JOHN ENSIGN,
U.S. SENATOR FROM NEVADA

Senator ENSIGN. Thank you, Mr. Chairman. It is great to be back on the Committee, by the way. We——

The CHAIRMAN. Glad to have you back, too.

Senator ENSIGN. This whole issue of privacy—and I think, first of all, some of it has been generated by the movies that we grew up watching and some of the books that we grew up reading, but, we live in the world today where some of those things are becoming reality.

I also think that some of this being generated by the Internet because people don't understand technology; they don't—they are afraid of it. A lot of this, it seems to me, is being put on the Internet which came out of telemarketing and mass mailing. I mean, that is where, people are sick of getting things in the mail, and—I know I am.

I will give you a great example, and I will compliment a company. I doubt if anybody from the Bose Company is here today, but I just bought one of those new Bose wave radios, and I was very impressed by the company, because at the register, they asked me if I wanted to sign up for the warranty information. I never fill those things out—I don't think anybody does hardly anymore—because they know that you are just getting put on some mailing list.

Well, right there, they gave an opt-out provision, and they said, "Do you want to be on our mailing list". And, of course, I said, "no".

But it is that type, I think, of thing that people are so sick of, that now this is being put on the Internet, that they think it is going to be much worse, and I think that—and what I would like your comment on, and I would like to start with you, Mr. Cate, is the idea that, first of all, people don't understand what they are trying to protect themselves from. Do they really understand—I mean, we all want—none of us want our personal identify to be stolen and somebody go get our credit cards, you know, and get a driver's license and go and ruin us. I mean, those are the horror stories that we hear about.

But at the same time—and I will use this example. I am from Nevada. You come and you stay in a hotel. You register in that hotel. You give them all of your information, including credit card information. That hotel now will periodically contact you and say, "We are having a special, a discount during a certain period of time". Well, you have signed up. You didn't necessarily opt in to get that information, but at the same time, you kind of like it. Some people might; some people might not.

And, you know, and the marketplaces determines whether or not companies are going to go more toward the opt-out or opt-in provision right up front. Because more and more people are demanding that.

But I guess what I would like your comment on is: How careful do we have to be that we don't ruin some of this interaction between a company that you have voluntarily given your information to and still protecting the privacy and getting the public to understand what privacy truly is?

Mr. CATE. Thank you, Senator. You have raised a number of issues. I think there is no question about what much of sort of the angst we see about the Internet that is called privacy might be somewhat more undifferentiated, and if you would do follow-up questions and surveys, you find that on the Internet, security seems to really be the major issue. I am not suggesting it is not related to privacy, but we should recognize that it is a very different issue.

What people are worried about, as I think Senator Boxer read out, is if I provide my credit card, will it be safe getting to you? And no amount of opt-in or opt-out or anything is going to do one thing about that, so if we want to respond to that concern, that should be identified more clearly.

It is also interesting that, of course, we, even people who spend a lot of time on the Internet or think we understand some little something about it, nevertheless find ourselves behaving somewhat, you know, irrationally. You know, will I provide my US Air—my Visa card to US Air when I buy a ticket online? You know, I worry, is it safe, but I provide it over the phone, or I provide it at a restaurant where the guy disappears with it for 20 minutes. I don't have any idea where it is, and I feel great. And, you know, it just shows that I am behaving like an idiot. I mean, that doesn't necessarily suggest that there should be legislation requiring that I be made to feel better.

On the question of sort of the interaction with companies, I think this does reflect the fact that although we all complain about junk mail, everybody does—it doesn't matter what side of this issue you are on; I have never anyone who didn't. On the other hand, it is interesting. If you talk to people in companies, the customer service center reports that the most frequent complaint letter they get related to direct mail is not, why did you send it, but why didn't you send it. My neighbor got a coupon; why didn't I. Why am I no longer getting the catalog in the mail? Why am I no longer getting these offers?

And the thing that we really don't like is anybody else getting something we didn't get. And so, you know, we have to worry about whether there really is much harm——

Senator ENSIGN. Not to interrupt you on that, but I haven't ever had anybody complain that they didn't get one of my mail pieces in a campaign.

[Laughter.]

Senator ENSIGN. Sorry.

Mr. CATE. There are so many things I should say to that, but none that I would, so—you know, so I think you are right and especially on the Internet, where the only relationship that most consumers have with their companies that they do business with is information. The only way my banker or airline company or whatever that I deal with online knows me is through information, so the only way they know what to offer me, what to show me, what meets my interest, is by collecting and using that information. To cut that off only hurts me.

Senator ENSIGN. Just before the other—and I want both of you to follow up. Also maybe incorporate being somewhat familiar with health information—I mean, that seems to be one of our most previous things that we want private, and we talk about balancing all of this. And yet if you are into the study of epidemiology, the spread of diseases, we know that what you don't want is your medical information made public, because those are private things you wouldn't want them to know. But—you also don't want to have somebody perhaps discriminate against you on a job if they find something out, or just some people are just real private about those kinds of things.

But at the same time, that information is very important for us when we are, you know, talking about especially communicable diseases or studying—for instance, in Nevada right now, there is this leukemia cluster going on with kids. Well, if you don't know that there are 11 cases, if that information isn't shared, we don't know that there is a leukemia cluster going on.

And so, just if you could, incorporate some of those thoughts into your response.

Mr. ROTENBERG. Senator, I need to say again that it is I don't think generally the view of the privacy community to oppose online marketing. I think the question is, how can you do it in a way that is fair, you know, and acceptable to consumers. Frankly, if you do it in a way that is not fair and acceptable, then you get a lot of backlash, and we have seen that.

Now, I said earlier that I think the right approach is opt-in coupled with opt-out, and in fact, in terms of the history of the Inter-

net, this is common sense to most people. If you want to get on a mailing list, if you want to receive information about a topic area, you subscribe to the list, and you get it for as long as you want, and if you are not happy about it or if you lose interest, you unsubscribe, and the relationship ends.

What a lot of the marketing companies try to do, in effect, is they said, "Oh, we are not really concerned if you are interested in this; we think you are interested in this; we are going to put you on the list, and we are going to make it difficult for you to get off the list". Now, I think in that kind of relationship, people understandably aren't going to be very happy, so what I think a good privacy law does is establish those practices that allow businesses and consumers to say, "OK, we all agree to this; I want to get that information, and this is going to be made to work".

And I think, of course, in the medical privacy area, it is particularly important to do that, as Eli Lilly learned this past week with their inadvertent mailing.

Mr. SCHWARTZ. Let me begin by saying something about health information. You are absolutely right that having anonymous information and good statistical data sets is critical to the nation's public health. This is something on which I have been privileged to work with Department of HHS. The Center for Disease Control and the National Center for Vital Health Statistics look at these issues very carefully to make sure that there are high-quality, statistical data sets for the nation's scientists to work with.

The second thing I would like to say is that I think what you are describing, Senator, is the development of a mass-market Internet. We have gotten there quickly. There are people who say that every year in Internet time is about 7 years off the Internet because everything changes so quickly. We have moved very quickly from a first generation Internet in which there were only scientists on it to now I don't know how many generations in which everybody is on it. I have to tell you personally this is something I have felt, because my mother a number of years ago decided to get a computer at home, and for a while, I felt like I was on full-time tech support in addition to teaching law and going about my life. So now everybody is on the Internet, and it is not surprising that Congress is thinking about consumer protection legislation.

And I think in the history of this country, as other devices such as the automobile, such as commercial aviation, move into the mass market, Congress has stepped in to try to stop some of the abuses.

Senator ENSIGN. Thank you, Mr. Chairman.

The CHAIRMAN. Very, very good. This has been an outstanding panel. The Committee is indebted to you, and we will leave it open for questions or any add-ons that you may have and your observations.

We have got to move now to panel number 2 as quickly as we can. We thank them for their patience. We have got Hans Peter Brondmo, author of "The Engaged Customer;" Les Seagraves, the vice president of Earthlink; Paul Misener, of Amazon, he is the vice president of global public policy; Jason Catlett, the president and founder of Junkbusters; and Ira Rubinstein, the associate general counsel of Microsoft.

And I realize the hour is getting late, and we are going to have—you see the interest of the Senators here, and we are going to have to give everyone just as much time as you possibly need. We will include the statements in their entirety in the record, and we will ask you if you can please summarize them in 5 minutes, so that will take the next half-hour here with this important panel.

Mr. Seagraves, are you ready?

STATEMENT OF LES SEAGRAVES, VICE PRESIDENT AND CHIEF PRIVACY OFFICER, EARTHLINK INC.

Mr. SEAGRAVES. Mr. Chairman and members of the Committee, I am the chief privacy officer for Earthlink. I appreciate this opportunity to speak to you about Earthlink, privacy, and legislation.

Earthlink, based in Atlanta, is the nation's second largest Internet service provider, connecting approximately 5 million customers to the Internet through dial-up, broad band, and wireless services. We have built our company and customer base over the last 7 years by providing fast, reliable connections and superior customer service and technical support.

Our focus on customer service has immersed us in the privacy debate. While we generate the majority of our revenue from monthly subscription fees, there is always the temptation, not to mention a compelling business case, to sell our valuable customer information to third parties. But early in our company's history, we decided to forego additional revenue we could make from selling our customers' personal information in exchange for gaining our customers' long-term trust by protecting their privacy.

This decision continues to be a tough one. On one hand, Earthlink stands on the threshold of renewed profitability with pressure from shareholders and the investment community to squeeze out every extra dollar we can, and with the devaluation of Internet advertising, merchants are increasingly willing to pay for targeted personal information.

On the other hand, we are an ISP with a strong focus on customer service. Our customers rely on us not only to give them fast, reliable Internet connections, but to help them enjoy the best possible online experience. If our customers have technical problems, they can use our tech support. To reduce spam, they look to us to provide both service-side and client-side filters. And regarding their personal information, they look to us to protect their privacy. We have gladly accepted this role and continue to garner high levels of customer satisfaction and loyalty.

As an ISP, we are not just running a web site. We have lots of detailed customer information that would be quite valuable to affiliates or partners or other third-party marketers. Opt-in versus opt-out really isn't an issue for us, because we don't share customers' personal information. Although our privacy policy may seem to be typical notice, choice, access, and security, the fact is Earthlink has chosen not to be in the business if selling, sharing, or renting customers' personally identifying information, and this is a huge distinction between Earthlink and many other companies that collect information online.

We believe that good privacy means good business. Trust equals revenue. Earthlink has highlighted privacy in its national adver-

tising campaign with great response. I think it is important to point out the forces that control Earthlink's actions and decisions on privacy today. First, a strong stance on privacy is just good business. On the outside, we are guided by the FTC privacy guidelines and Section 5 of the FTC Act. On the inside, we do what we say we are going to do. This is one of the core values and beliefs developed by former Earthlink chairman and MindSpring founder, Charles Brewer. If we make a huge privacy mistake, we would be severely penalized by the press, our customers, and the market.

Under most of the pending and proposed Federal legislation in Congress today, Earthlink probably already complies without making any changes. We have a solid privacy policy. We notify customers of the information we collect, and although we say we give customers a choice of sharing their information, so far we have not asked to make that choice. Customers can access their information 24 hours a day. Our network security involves some of the most advanced practices in the industry.

Federal legislation would have certain benefits. It could set a much needed Federal standard for privacy policies and practices. It could preempt state law, eliminating the need for Earthlink to navigate 50 different state privacy laws. It would also help to weed out those companies that abuse the privacy of consumers.

Congress should exercise care not to create a regulatory mine field for good companies like Earthlink that do their best to comply. Legislative requirements should not prevent us from clearly and effectively communicating with our customers about their privacy and choices. Legislation should not strain the ability of Government by enforcing broad laws that focus on technical compliance rather than on actual harm to consumers.

Most of our customers want to take advantage of the convenience and the innovation that the Internet provides. They want to get the best prices for the merchandise and services. They don't want to have to log in to every web site. They want an Internet that is customized to their tastes and preferences. They also want protection from fraud and misuse of their information. Our customers would benefit from the creation of a standard that clearly gives them the information they need to make intelligent decisions about their own privacy.

By encouraging the same technical innovation that brought us the Internet, Congress can rely on the private sector as a partner in protecting privacy. If you must pass privacy legislation, focus on setting a standard, not creating regulatory barriers. Focus on getting customers meaningful information they really need to make decisions. Focus on helping good companies like Earthlink provide services that people really want and use and thereby drive the economy.

Thank you again for the opportunity to testify.

The CHAIRMAN. Thank you, sir.

[The prepared statement of Mr. Seagraves follows:]

PREPARED STATEMENT OF LES SEAGRAVES, VICE PRESIDENT AND CHIEF PRIVACY OFFICER, EARTHLINK, INC.

Mr. Chairman and Members of the Committee: My name is Les Seagraves and I am the Chief Privacy Officer for EarthLink. I appreciate this opportunity to speak to you about EarthLink, privacy and legislation.

EarthLink, based in Atlanta, is the nation's 2nd largest Internet Service Provider, connecting approximately 5 million customers to the internet through dial-up, broadband and wireless services. We have built our company and customer base over the last 7 years by providing fast, reliable connections and superior customer service and technical support.

Our focus on customer service has immersed us in the privacy debate. While we generate the majority of our revenue from monthly subscription fees, there is always the temptation, not to mention a compelling business case, to sell our valuable customer information to third parties. But early in our company's history we decided to forgo the additional revenue we could make from selling our customers' personal information in exchange for gaining our customers' long term trust by protecting their privacy.

This decision continues to be a tough one. On one hand, EarthLink stands on the threshold of renewed profitability with pressure from shareholders and the investment community to squeeze out every extra dollar we can. And with the devaluation of internet advertising, merchants are increasingly willing to pay for targeted personal information.

On the other hand, we are an ISP with a strong focus on customer service. Our customers rely on us not only to give them fast, reliable internet connections, but to help them enjoy the best possible online experience. If our customers have technical problems, they can use our award-winning technical support. To reduce spam, they look to us to provide both server-side and client-side filters. And regarding their personal information, they look to us to protect their privacy. We have gladly accepted this role and continue to garner high levels of customer satisfaction and loyalty.

WHY IS EARTHLINK DIFFERENT?

As an ISP, we're not just running a website. We have lots of detailed customer information that would be quite valuable to "affiliates" or "partners" or other third-party marketers. Opt-in versus opt-out really isn't an issue for us because we don't share customers' personal information. Although our privacy policy may seem to be the typical notice, choice, access and security, the fact is that EarthLink is not in the business of selling, sharing or renting customers' personally identifying information. This is a huge distinction between EarthLink and many other companies that collect online information. We believe that good privacy means good business. Or put another way, trust equals revenue. EarthLink has highlighted privacy in its national advertising campaign with great response.

While we believe that our current privacy policy meets industry best practices, we are currently working on a new privacy policy which should set an example for proper clarity and scope. We will, in clear plain language, explain how and what information we collect, what we do with it and what a customer can do to protect their information. We have developed the following privacy principles as an internal guide to our day to day business activity:

1. We will let our customers know all of the personal information that we collect and what we do with it.

2. We will not give, sell or share personally identifying information to anyone except to:

- comply with valid law enforcement requests for information
- deliver our service to our customers
- honor agreements where customers come to us through third-party promotions.

3. No one else will use the information that our customers give to us to contact our customers except on our behalf.

4. Our customers will be able to choose what non-essential information they provide to us.

5. Our customers will be able to choose how we contact them.

6. Our customers will have access to all of their personal information.

7. We will take care to secure all customer information that we have.

8. We will insure that all of our partners and contractors abide by and agree to these principles.

WHY IS EARTHLINK DOING THIS?

I think it is important to point out the forces that control EarthLink's actions and decisions on privacy today. First, a strong stance on privacy is just good business. On the outside we are guided by the FTC privacy guidelines and Section 5 of the FTC Act. On the inside we do what we say we are going to do, this is one of the Core Values and Beliefs developed by former EarthLink Chairman and MindSpring

founder Charles Brewer. If we make a huge privacy mistake, we would be severely penalized by the press, our customers and the market.

WHAT WOULD BE THE ADVANTAGES TO EARTHLINK IF FEDERAL LEGISLATION PASSED?

Under most of the pending and proposed Federal legislation in Congress today, EarthLink probably already complies without making significant changes. We have a solid privacy policy. We notify customers what information we collect. Although we say we give customers a choice of sharing their information, so far we have not asked them to make the choice. Customers can access their information 24 hours a day through the internet or the telephone. Our network security involves some of the most advanced practices in the industry.

WHAT WOULD BE THE ADVANTAGES TO EARTHLINK IF FEDERAL LEGISLATION PASSED?

Federal legislation would have certain benefits. It could set a much needed Federal standard for privacy policies and practices. It could preempt state law, eliminating the need for EarthLink to navigate 50 different state privacy laws. It would also help to weed out those companies that abuse the privacy of others.

WHAT ARE EARTHLINK'S CONCERNS ABOUT LEGISLATION?

Congress should exercise care not to create a regulatory minefield for good companies like EarthLink that do their best to comply. Legislative requirements should not prevent us from clearly and effectively communicating with our customers about their privacy. Legislation should not strain the ability of government by enforcing broad laws that focus on technical compliance rather than the actual harm to consumers.

In the media, much of the debate about privacy legislation seems to focus on opt-in versus opt-out provisions. While important, these provisions should be viewed in their proper context as part of the single information practice of notice. And we should all recognize that no standard is foolproof. Even with the stricter opt-in standard, if the boxes on the screen are already checked, is it still opt-in? With either an opt-in or an opt-out standard, the bottom line is to ensure customer notice and consent.

We should further note that any proposed new privacy legislation would not be the first. Congress has a long history of enacting laws that address the use of personal information, including the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Children's Online Privacy Protection Act (COPPA), the Electronic Communications Privacy Act (ECPA), and many others.

However, Congress should also be aware of the unintended consequences that can result from even the best intentioned legislation. While few would argue with the goal of COPPA to prevent the collection of information from young minors, the cost of compliance proved to be too great for many legitimate, independent, local kid-oriented websites. In an online world where an increasing amount of web traffic is concentrated in a relative handful of sites owned by large media and software companies, privacy protection should not further reduce diversity on the World Wide Web.

HOW WOULD LEGISLATION EFFECT EARTHLINK'S CUSTOMERS?

Most of our customers want to take advantage of the convenience and innovation that the internet provides. They want to get the best prices for merchandise and services. They don't want to have to log in to every web site. They want an internet that is customized to their tastes and preferences. They also want protection from fraud and misuse of their information. Our customers would benefit from the creation of a standard that clearly gives them the information they need to make intelligent decisions about their own privacy. By encouraging the same technical innovation that brought us the internet, Congress can rely on the private sector as a partner in protecting privacy.

CONCLUSION: SUGGESTIONS TO LAWMAKERS

If you must pass privacy legislation, focus on setting a standard not creating regulatory barriers. Focus on getting customers meaningful information they really need to make decisions. Focus on helping good companies like EarthLink provide services that people really want and use and thereby drive the economy.

Thank you again for the opportunity to testify.

* * * * * * *

EARTHLINK CORE VALUES AND BELIEFS

What's important at EarthLink? We are convinced that the key to creating a truly great organization is an intense focus on the values that guide its people's actions. These are EarthLink's "Core Values and Beliefs". If we don't seem to be living up to them, call us on it!

- We respect the individual, and believe that individuals who are treated with respect and given responsibility respond by giving their best.
- We require complete honesty and integrity in everything we do.
- We make commitments with care, and then live up to them. In all things, we do what we say we are going to do.
- Work is an important part of life, and it should be fun. Being a good businessperson does not mean being stuffy and boring.
- We love to compete, and we believe that competition brings out the best in us.
- We are frugal. We guard and conserve the company's resources with at least the same vigilance that we would use to guard and conserve our own personal resources.
- We insist on giving our best effort in everything we undertake. Furthermore, we see a huge difference between "good mistakes" (best effort, bad result) and "bad mistakes" (sloppiness or lack of effort).
- Clarity in understanding our mission, our goals, and what we expect from each other is critical to our success.
- We are believers in the Golden Rule. In all our dealings we will strive to be friendly and courteous, as well as fair and compassionate.
- We feel a sense of urgency on any matters related to our customers. We own problems and we are always responsive. We are customer-driven.

The CHAIRMAN. Mr. Brondmo.

STATEMENT OF HANS PETER BRONDMO, AUTHOR, "THE ENGAGED CUSTOMER" AND NETCENTIVES, INC. FELLOW

Mr. BRONDMO. Chairman Hollings, members of the Committee, I thank you for inviting me to participate in this very important hearing about Internet privacy.

I am a technology entrepreneur. I am an author, and I am a consultant to industry on the usage of customer information and email to build customer relationships. The company I founded in 1996, NetCentives, today manages over 50 million relationships with customers. It manages customer information, opt-in and opt-out, on over 50 million people on behalf of some of the leading corporations in this country.

At the center of the debate about Internet and privacy is a very simple question. Who owns information about an individual? Does a person have rights to and control of the information being gathered about him or her? Or should whoever collects the information be able to use and commercially exploit that information in any manner they see fit?

My remarks this morning will revolve around this broader issue of information ownership, specifically how we think about collecting and using personally identifiable information consistent with our beliefs both in personal liberty and in free enterprise. I begin by suggesting that we consider personal information to be a capital asset, just like we do financial information.

It goes without saying that no modern business survives today in a fiercely competitive marketplace if it keeps its financial assets in disarray, not knowing how much working capital is available, and not knowing who is managing the money. Yet that is exactly how most companies manage their customer information assets today. They don't know what they have got; they don't know who

has got what; and they don't know what data bases contain what information.

It turns out that a comparison between financial assets and information assets provides a powerful model for thinking about information ownership. To illustrate this, let's consider the following familiar example from the banking world.

Like many Americans, I have some savings, and I have a stock portfolio. I have chosen to hand over control of my financial assets to professional asset managers. I keep my money in a local bank, and I work with a stockbroker. When selecting my bank and stockbroker, I have two primary selection criteria: trust and returns. If I do not trust a bank, I will not give them my money, and if the competition, the bank next door, consistently out-performs and offers better returns, what will I do? I will withdraw my money, and I will deposit it with the bank next door, with the competition.

As individuals, I believe that we are increasingly becoming aware that our personal information also has value, and just as we will choose to deposit our financial assets with asset managers based on trust and returns, we are learning to apply the same two criteria when we deposit our personal information with a business, and if that business breaches our trust or does not manage our information in order to generate a return in the form of good service, convenience, what will we do? We will withdraw it, and we will deposit it with a competitor who does.

In short, the expectation is that we own and control our personal information. Yet while the individual may own the information about themselves, we must also realize that it is this information when used properly which enables businesses to build relationships with its current and prospective customers, and to realize significant financial gain from its ongoing interactions with those customers.

Without access to personally identifiable information, companies cannot get to know their prospects and customers, and if they cannot know and enter into personal dialog with these very people they do business with, it is equivalent to not being able to greet a customer when she first walks into your store, or even worse, not being able to develop a relationship with that customer and recognize her for her loyalty when she returns to that store over and over again.

Yet does the customer want the store to know her before she has even introduced herself? Does walking into a store for the first time constitute some implicit permission for the store to dip into a data base and look up who she is? Would she be comfortable if the grocery store knew how many children she has the very first time she entered? Would she be concerned if the grocer sold their knowledge about her low-fat diet to her insurance provider without explicit permission?

The issue is one of personal choice about personal data, and these are exactly the questions we are debating when we are discussing notice, choice, access, and security.

In summary, the new thinking that must be adopted in order to realize the potential value and benefits inherent in the smart use of customer information is based on the following two principles: first, that the individual owns and controls his or her personal in-

formation and chooses to deposit that information with companies based on expectations of trust and returns; second, that businesses represent themselves as the custodians, not the owners, of personal information. They invest in and actively manage that information asset in order to generate returns for the customers and for their shareholders.

To ensure broad adoption of these principles, I believe that government regulation is necessary. While it is not the role of Government to dictate to companies what they may do with information nor what information they may collect, it is the responsibility, in my view, of the Federal Government as an extension of its constitutional duty to protect civil liberties, to ensure that the use of information is based on clear notice, consent, and always under the control of the individuals to who it belongs.

Mr. Chairman, members of the Committee, change is always difficult. As we all know, it is difficult at the personal level, and it can be painful and sometimes expensive at the corporate level. When change came to the auto industry a few decades ago, it was resisted, not embraced. We all know the consequences. It is in my humble opinion time for all corporate America to change the way it uses and manages customer information. Leaders who embrace this change will stand to win big. Those who resist it will be left behind.

I am encouraged by your leadership in this area, and thank you for the opportunity to address the Committee this morning.

The CHAIRMAN. We thank you.

[The prepared statement of Mr. Brondmo follows:]

PREPARED STATEMENT OF HANS PETER BRONDMO, AUTHOR, "THE ENGAGED CUSTOMER" AND NETCENTIVES, INC. FELLOW

Chairman Hollings, Senator McCain and Members of the Committee thank you for inviting me to participate at this important hearing on Internet privacy. My name is Hans Peter Brondmo and I am a technology entrepreneur, author and consultant to industry on the usage of customer information and email to build customer relationships. I believe that these hearings are timely because we find ourselves at a fork in the road where one path can lead us to a win both for individual rights and for industry, while the other takes us down a treacherous path where all parties loose. Strong leadership and decisive action will ensure that we choose the correct path.

At the center of the debate about Internet and privacy is a simple question: Who owns information about an individual? Does each person have rights to and control of the information being gathered about him or her or should whoever collects the information be able to use and commercially exploit it in any manner they see fit? While the question may be simple the answers are complex.

My remarks today focus on the broader issue of information ownership in which I propose a framework for how we think about collecting and using personally identifiable information, consistent with our belief both in personal liberty and in free enterprise. I will return to this framework momentarily. First let me take a brief look at where we find ourselves at this moment in time.

It seems that historically the rules which govern what information a company can collect about its customers and prospects and what they can do with this information favors industry over individual rights. For example, there have been egregious instances in which many a credit worthy individual has been summarily denied a home mortgage, auto loan or educational financing on the basis of incorrect personal data that had been surreptitiously collected and never submitted to the person for verification. Erroneous data often has been through the hands of several firms without the individual's knowledge, making correction impossible. Meanwhile, without effective recourse, a deserving individual's personal life is severely damaged.

The attitude that dominates the current business environment is that Federal privacy legislation will hamper free enterprise and limit industry's ability to grow and

innovate. I disagree with this attitude and believe that we need to move away from the mindset that any information a company captures about their customers is theirs to exploit and even sell in whatever manner they see fit. I would like to propose that industry allows the free market to determine the value of their integrity. If customers trust the organizations they do business with and these businesses have integrity, customers will award them with access to their personal information. If not, it seems only reasonable that a customer must be allowed to inspect or withdraw that information. An obvious question is why now? If we have managed so far, why can we not continue on the same program? And the answer is obvious—The Internet. According to what we read, every device and tool we rely on to enhance our lives will soon be connected to the Internet: our automobiles, our homes, our cellular telephones, our television sets, our hand-held cameras, our Jacuzzi tub, our electronic credit card. And while the benefits are many including pervasive access to information and the ability to communicate regardless of location, there is a dark side. These devices will pass along information about who is using them, where they are located and perhaps even details about what a person is doing. This information about individuals can be collected and analyzed in ways that were not possible prior to the Internet. The potential threats to privacy are enormous.

While the new technologies present fantastic opportunities and real threats to individual rights it is also important to recognize that the challenges posed to industry are real and formidable as well. Internet technologies are changing the manner in which companies conduct commerce. They are fundamentally impacting the way businesses communicate with and service their customers. It's a fact that personally identifiable information is a key ingredient to individualized and successful commerce in an information economy. Just as fossil fuels powered the industrial revolution and new transportation technologies made it possible to achieve economies of scale, information is the fuel of the global economy and the Internet is the engine powering an explosive growth. My experience has convinced me that if the ability to collect and use customer information is compromised, American industry will be at a competitive disadvantage. That said, business as usual will not do.

While some industry leaders are holding themselves to high standards, a majority of businesses still think in old terms regarding how to realize value from personally identifiable information. Corporations needs to come to terms with a new definition of the value they realize from such information both in order to safeguard personal liberties and in order to realize the vast potential of properly managed information.

Central to this definition of value are two *assumptions*: first that customer information is a precious capital asset and second, that the individual, not the company they do business with owns and controls information about themselves.

Acting on these two assumptions, let me return to the framework that I made earlier reference to. It goes without saying that no modern business survives long in today's fiercely competitive marketplace if it keeps its financial assets in disarray not knowing how much working capital is available and who has the money. Yet that's exactly how most companies manage their customer information. They don't know what they've got, they don't know who has what and they don't know what databases contain what information. It turns out that the comparison between financial capital and information capital is a good way to illustrate the new framework. Consider the following familiar example from the banking industry.

Like most Americans, I have money in the bank and I have a stock portfolio. I have chosen to hand over my financial assets to professional asset managers. I keep my money in a local bank and a I work with a stockbroker. When selecting my bank and stockbroker I had two primary selection criteria: TRUST and RETURNS. If I do not trust a bank I will not give them my money. And if the competition, the bank next door, consistently offers better returns what will I do? I will withdraw my money from my current bank and deposit it with the competition.

As individuals we are increasingly becoming aware that our personal information has real value. And just as we will choose to deposit our financial assets with asset managers based on TRUST and RETURNS, we are learning to apply the same two criteria when we "deposit" our personal information with a company. And if that company breaches our trust or does not manage our information in order to generate a return in the form of good service and convenience, we will withdraw it and deposit it with a competitor who does.

Information that an organization collects about the individuals it interacts with should be treated like a capital asset. It is this information, when used properly, which enables a company to build relationships with their current and prospective customers and to realize significant financial gain from its ongoing interactions with those customers. Without access to personally identifiable information companies cannot get to know their prospects and customers. And if they cannot know and enter into a personalized dialogue with the very people they do business with, it is

equivalent to not being able to greet a customer when she walks into a store. Or even worse, not being able to develop a relationship with that customer and recognize her for her loyalty when she returns to that store over and over again.

Yet does the customer want the store to know who she is before she has introduced herself? Does walking into a store for the first time constitute implicit permission for the store to dip into a database and look up who she is? Would she be comfortable if a grocery store knew how many children she has the very first time she entered? Would she be concerned if the grocer sold their knowledge about her low-fat diet to her insurance provider without her permission and knowledge? The issue is one of personal choice about personal data. And these are the types of questions we are asking when we discuss "opt-in" policies, notice and access.

To address these important concerns, I offer four principles that exemplify the new thinking I believe must be adopted in order to realize the potential value and benefits inherent in the smart use of customer information.

- Organizations (data vendors) represent themselves as the custodians—not owners, of personal information
- Organizations invest in and actively manage the information they gather about individuals in order to generate a return to those individuals as well as to all other constituents (shareholders)
- The individual owns and controls his or her personal information and chooses to deposit it with a company based on expectations of TRUST and RETURNS.
- Individuals receive many benefits such as better service and more relevant information, timesavings and achieve higher efficiencies as an organization gets to know them by collecting and appropriately utilizing personal information about them.

While the argument that industry self regulation can address all these principles may seem appealing, it is my belief that unless we have uniform and consistent rules providing a foundation for these principles the individual cannot rely on for protection and consistency. Furthermore it means we do not have a level playing field for industry.

Let me share with you an example that illustrates some common misconceptions and hurdles that confront those who favor giving customers proper notice, access and control of their personal information. And while this example illustrates a company that did the right thing in the end, it also illustrates that doing right by the customer is doing right by the business and therefore that appropriately written legislation will have a net positive impact on business.

The email marketing company I founded in 1996 has worked for several years with an online music retailer. Some time ago the retailer was experiencing a customer satisfaction problem because they were sending too many promotional emails to their customers. Once you had made a purchase from the company you were added to their marketing database and began receiving electronic commercials. It was very difficult to stop the flood. We argued for better notice and a simple and straightforward unsubscribe mechanism, making it easy for customers to remove their name from the mailing list. The company hesitated to heed our advice for seemingly logical reasons: They had spent tens of millions of dollars on marketing to attract their customers and we were telling them that if a customer wanted to disengage, it should not only be possible, it should be easy. They could not convince themselves that "letting a customer go" was good business. As their satisfaction problems continued to grow the music retailer finally decided to perform a test with a small sub-segment of their customers. They implemented a very simple one-click unsubscribe process for the test-customers making it easy for them to stop the emails or modify their personal profile. To the retailer's great surprise, they discovered that their new process had no negative impact on the business whatsoever. The people that complained about receiving too many emails were not likely to make any more purchases. More astonishing was the fact that when the company rolled out the new functionality to their whole customer base and promoted on their e-commerce web-site how easy it was to opt-out, their level of opt-in improved significantly. People were more comfortable signing up when they knew they were in control and it would be easy to disengage from the service should they not want it in the future. Providing customers with the ability to easily access and change their personal profile information, including removing their names altogether built trust and confidence. The music retailer profited from making it easy for its customers to unsubscribe or disengage.

As this example illustrates determining what is appropriate notice and what represents adequate permission in order to collect personally identifiable information is not simple. Furthermore it would also seem that there is no single solution appropriate for all situations. My experience has convinced me that opt-out with notice may be an appropriate level of protection in many instances. Yet there are also

many cases where strict opt-in is the only appropriate solution. In situations where information is being collected strictly for internal use in an organization, my opinion is that an appropriate level of protection is afforded by requiring opt-out with notice. Where there may be possibilities that personally identifiable information will be transferred to an external organization that an individual is interacting with, it seems the only appropriate solution is to require full opt-in.

What is key here is the concept that no matter the circumstance, every firm must assume full responsibility for protecting personal data entrusted to it, whether by customers, employees or prospects. Implementation will necessarily vary with circumstances but as in matters of law, policies will indicate intent.

Finally we must acknowledge the considerable cost to industry implicit in requiring stricter enforcement of notice, permission and complete access to and control of personal information. In my opinion the requirement that industry provides individuals with access to and control of personally identifiable information will be the most costly component to implement as it probably requires that such information be centralized.

Most organizations do not have the technical ability to centralize their customer information today, nor do they have the internal processes to enforce uniform and appropriate use of customer information. That said, it is feasible to implement such solutions with existing technology and developing best practices business processes to support such an initiative is a question of good management. Furthermore, the policy changes an organization must undertake to implement proper privacy protection for its members and customers are the same initiatives essential to focusing the organization around its customers, an important trend in business and marketing. In other words, the investment made to protect the individuals' privacy, is an investment in best business practices and will generate handsome returns when made a corporate priority.

America is a country of innovators and inventors. The way personally identifiable information is managed by industry must change and I am convinced that the spirit of innovation and creativity will lead us to new and significantly enhanced solutions. I have no doubt we can create options that support industry's need to collect, combine and even share personally identifiable information, all without compromising individual privacy.

In order to drive this change, I believe that government regulation is necessary. While it is not the role of government to dictate to companies what they may do with customer information, it is the responsibility of the Federal government as an extension of its constitutional duty to protect civil liberties to ensure that the use of information is based on the consent and always under the control of the individuals to whom it belongs. We need a foundation for major change as well as a level playing field and only Federal legislation can establish the required ground rules. While industry self-regulation can work in some cases and in some states, it will not be an effective way to ensure that a win-win scenario for the all citizens of America and for industry alike. When it comes to protecting privacy and empowering a competitive data industry, the Federal government, in my opinion, has an indispensable role to play.

Mr. Chairman, and Members of this Committee I am encouraged by your leadership in this area and thank you for the opportunity to address the committee this morning.

The CHAIRMAN. Mr. Misener.

STATEMENT OF PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM

Mr. MISENER. Thank you, Chairman Hollings, very much, and members of the Committee. My name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy.

Mr. Chairman, Amazon.com is pro-privacy. The privacy of personal information is important to our customers, and thus it is important to us. Indeed, as Amazon.com strives to be Earth's most customer-centric company, we must provide our customers the very best shopping experience, which is a combination of convenience, personalization, privacy, selection, savings, and other features.

At Amazon.com, we manifest our commitment to privacy by providing our customers notice, choice, access, and security. Ama-

zon.com was one of the very first online retailers to post a clear and conspicuous privacy notice, and last summer, we proudly unveiled our updated and enhanced privacy policy by taking the unusual step of sending email notices to all of our customers, then totaling well over 20 million.

We also provide our customers meaningful privacy choices. In some instances, we provide opt-out choice, and in other instances, we provide opt-in choice. We are an industry leader in providing our customers access to the information we have about them. They may easily view and correct as appropriate their contact information, payment methods, purchase history, and even the click stream record of products they view while browsing Amazon.com's online stores.

Finally, Amazon.com vigilantly protects the security of our customers' information. Not only have we spent tens of millions of dollars on security infrastructure; we continually work with law enforcement agencies and industry to share techniques and develop best practices. It is very important to note that other than obligation to live up to pledges made in our privacy notice, there is no legal requirement for Amazon.com to provide our customers the privacy protections that we do.

So why do we provide notice, choice, access and security? The reason is quite simple. Privacy is important to our customers, and thus it is important to Amazon.com. We simply are responding to market forces. Indeed, if we don't make our customers comfortable shopping online, they will shop at established brick-and-mortar retailers who are our biggest competitors. These market realities lead us to conclude that there is no inherent need for privacy legislation.

That said, we have been asked whether Amazon.com could support a privacy bill. Perhaps we could, Mr. Chairman, but only under certain circumstances. Under no circumstances would we support a state or local law governing online privacy. Not only would such laws be constitutionally suspect, a nationwide web site like Amazon.com would find it difficult, if not impossible, to comply with 50 or more sets of conflicting rules.

At the Federal level, Amazon.com could support a bill that would require notice and meaningful choice, but only if it would preempt inconsistent state laws, bar private rights of action, and address both online and offline activities. Please allow me to briefly address each of these points.

First, any Federal privacy legislation applied to online activities must preempt inconsistent state laws. Even though such laws most likely would fail a constitutional challenge, the expense and uncertainty of litigation should be avoided with a congressionally adopted ceiling.

Second, Amazon.com could support a privacy bill only if it would bar private rights of action. The threat of aggressive private litigation would cause companies to balkanize their privacy notices for the sake of legal defensibility at the expense of simplicity and clarity. Ten-page privacy statements in fine print legalese would become the norm.

A regulatory body such as the Federal Trade Commission, on the other hand, could balance the competing interests of legal precision

and simplicity. A class action plaintiff's lawyer would have no such motivation.

Third and finally, Amazon.com believes that privacy legislation must apply equally to online and offline activities. It makes little sense to treat information collected online differently from the same and often far more sensitive information collected through other media, such as mail and warranty registration cards, point of sale purchase tracking, and magazine subscriptions.

On the one hand, such parity is necessary in fairness to online companies, but more importantly, it would be misleading to American consumers to enact a law that applies only to online entities, because for the foreseeable future, the putative protections of such a law would apply only to a tiny fraction of consumer transactions. Last year, online sales accounted for less than 1 percent of retail business.

Obviously any law that addresses only online transactions could not benefit consumers much at all, compared to one that equally addresses online and offline activities. Moreover, to the extent it provides real consumer benefits, a law that addresses only online activities would have the perverse effect of failing to provide any benefits to those on the less fortunate side of the digital divide. Indeed, consumers who, because of economic situation, education or other factors are not online would receive no benefits from a new online-only law.

In sum, Mr. Chairman, Amazon.com is pro-privacy in response to consumer demand and competition. We believe market forces are working and thus believe there is no inherent need for legislation. Nonetheless, Amazon.com could support limited Federal legislation, but only if it preempts state laws, only if it bars private rights of action, and only if it applies to offline as well as online activities.

Thank you again for inviting me to testify, Mr. Chairman. I look forward to your questions.

The CHAIRMAN. Thank you very much.

[The prepared statement of Mr. Misener follows:]

PREPARED STATEMENT OF PAUL MISENER, VICE PRESIDENT, GLOBAL PUBLIC POLICY, AMAZON.COM

Chairman Hollings, Senator McCain, and members of the Committee, my name is Paul Misener. I am Amazon.com's Vice President for Global Public Policy. Thank you for inviting me to testify today.

A pioneer in electronic commerce, Amazon.com opened its virtual doors in July 1995 and today offers books, electronics, toys, CDs, videos, DVDs, kitchenware, tools, and much more. With well over 30 million customers in more than 160 countries, Amazon.com is the Internet's number one retailer.

Mr. Chairman, Amazon.com is pro-privacy. The privacy of personal information is important to our customers and, thus, is important to us. Indeed, as Amazon.com strives to be Earth's most customer-centric company, we must provide our customers the very best shopping experience, which is a combination of convenience, personalization, privacy, selection, savings, and other features.

At Amazon.com, we manifest our commitment to privacy by providing our customers notice, choice, access, and security. Please allow me to address each briefly:

Notice. Amazon.com was one of the first online retailers to post a clear and conspicuous privacy *notice*. And last summer, we proudly unveiled our updated and enhanced privacy policy by taking the unusual step of sending email notices to all of our customers, then totaling over 20 million people.

Choice. We also provide our customers meaningful privacy *choices*. In some instances, we provide opt-out choice, and in other instances, we provide opt-in choice. For example, Amazon.com will share a customer's contact information with our trusted partner Greenlight.com only after that customer makes an opt-in choice.

Access. We are an industry leader in providing our customers *access* to the information we have about them. They may easily view and correct as appropriate their contact information, payment methods, purchase history, and even the "clickstream" record of products they view while browsing Amazon.com's online stores.

Security. Finally, Amazon.com vigilantly protects the *security* of our customers' information. Not only have we spent tens of millions of dollars on security infrastructure, we continually work with law enforcement agencies and industry to share security techniques and develop best practices.

It is very important to note that, other than an obligation to live up to pledges made in our privacy notice, there is no legal requirement for Amazon.com to provide our customers the privacy protections that we do.

So why do we provide notice, choice, access, and security? The reason is simple: privacy is important to our customers, and thus it is important to Amazon.com. We simply are responding to market forces.

Indeed, if we don't make our customers comfortable shopping online, they will shop at established brick and mortar retailers, who are our biggest competition. Moreover, online—where it is virtually effortless for consumers to choose among thousands of competitors—the market provides all the discipline necessary. Our customers will shop at other online stores if we fail to provide the privacy protections they demand.

These market realities lead us to conclude that there is no inherent need for privacy legislation. That said, we have been asked whether Amazon.com could support a privacy bill. Perhaps we could, but only under certain circumstances.

Under no circumstances would we support state or local laws governing online privacy. Not only would such laws be constitutionally suspect, a nationwide website like Amazon.com would find it difficult if not impossible to comply with fifty or more sets of conflicting rules.

At the Federal level, Amazon.com could support a bill that would require notice and meaningful choice, but only if it would preempt inconsistent state laws, bar private rights of action, and address both online and offline activities. Please allow me to briefly address each of these points.

Preempt State Law. First, any Federal privacy legislation applied to online activities must preempt inconsistent state laws. As I noted earlier, it would be virtually impossible for a nationwide website to comply with inconsistent rules from multiple jurisdictions. Even though such laws most likely would fail a constitutional challenge, the expense and uncertainty of litigation should be avoided with a Congressionally adopted ceiling.

Bar Private Rights of Action. Second, Amazon.com could support a privacy bill only if it would bar private rights of action. The threat of aggressive private litigation would cause companies to balkanize their privacy notices for the sake of legal defensibility, at the expense of simplicity and clarity. Ten-page privacy statements and fine-print legalese would become the norm. A regulatory body such as the Federal Trade Commission, on the other hand, could balance the competing interests of legal precision and simplicity. A class action plaintiffs' lawyer would have no such motivation.

In addition, the aforementioned uniformity necessary to run nationwide websites would be destroyed by a host of trial lawyers suing companies all across the country. A single authority, such as the FTC, could provide the nationwide approach that private litigation cannot.

Parity with Offline Activities. Third, and finally, Amazon.com believes that privacy legislation must apply equally to online and offline activities, including the activities of our offline retail competitors. It makes little sense to treat information collected online differently from the same—and often far more sensitive—information collected through other media, such as offline credit card transactions, mail-in warranty registration cards, point-of-sale purchase tracking, and magazine subscriptions.

On one hand, such parity is necessary in fairness to online companies. It simply would not be equitable to saddle online retailers with requirements that our brick-and-mortar or mail order competitors do not face.

But more importantly, it would be misleading to American consumers to enact a law that applies only to online entities because, for the foreseeable future, the putative protections of such a law would only apply to a tiny fraction of consumer transactions. Last year, online sales accounted for less than one percent of all retail business. Obviously, any law that addresses only online transactions could not benefit consumers much at all compared to one that equally addresses online and offline activities such as using a grocery store loyalty card or subscribing to a magazine.

Moreover, to the extent it provides real consumer benefits, a law that addresses only online activities would have the perverse effect of failing to provide any bene-

fits to those on the less fortunate side of the digital divide. Indeed, consumers who, because of economic situation, education, or other factors, are not online would receive no benefits from a new, online-only law.

In sum, Mr. Chairman, Amazon.com is pro-privacy in response to consumer demand and competition. We believe market forces are working and, thus, believe there is no inherent need for legislation. We firmly oppose the adoption of any non-Federal privacy law that addresses online activities. Nonetheless, Amazon.com could support limited Federal legislation, but only if it preempts state laws, only if it bars private rights of action, and only if it applies to offline as well as online activities.

Thank you again for inviting me to testify, I look forward to your questions.

The CHAIRMAN. Mr. Catlett.

STATEMENT OF JASON CATLETT, PRESIDENT AND CEO, JUNKBUSTERS CORP.

Mr. CATLETT. Thank you, Mr. Chairman. It is an honor to appear before you again, and I would like to commend the Committee on its steadfast attention to privacy, particularly Senators Wyden and Burns for their hard work on junk email. Rather than reading a prepared statement today, I would like to comment on some of the examples that you have raised.

Gramm-Leach-Bliley, I think, serves as an excellent example of the utter failure of the opt-out model. A survey by the American Banking Association found that 41 percent of people do not recall having received their notices, so their privacy interests do not seem to be protected by this.

We could take an example of one of these privacy notices, which are very confusing and, in my opinion, highly deceptive in some cases. Let's take U.S. Bancorp's consumer privacy pledge which opens with the sentence, "Protecting your privacy is important to the U.S. Bancorp family of financial service providers."

If you read 400 words down, you will then find that the bank allows itself to disclose all of the information it has to other financial institutions with which it has joint marketing arrangements. Indeed, according to the state attorney general of Minnesota, Mike Hatch, the company has a history of making such disclosures.

He alleges that U.S. Bank has disclosed the following information, which is in my written testimony: name, address, telephone numbers, gender, marital status, home ownership status, occupation, checking account number, credit card number, Social Security number, birth date, account open date, average account balance, automated transactions authorized, credit card type and brand, number of credit cards, cash advance amount, behavior score, bankruptcy score, date of last payment, amount of last payment, date of last statement, statement balance.

Now, in its defense, the CEO of the bank characterized this kind of transaction as an industry-wide practice, and as the bank's privacy statement discloses, it can continue to do this. Now, I think if you were to ask the average American consumer, is she happy about having all of this information sold to a telemarketer, I think we can assume that she would say "no". And yet her interests and wishes are not being served by the opt-out model. She has to find the statement, read it, go through the opt-out procedure, and under the limited rights provided by Gramm-Leach-Bliley, can't even opt out of many of the uses of information.

So I think this example shows that opt-in is the appropriate standard. If the bank wishes to be able to sell information about

its customers, it can offer them a month's free checking in return and obtain their permission. That is the appropriate standard in my view.

Another example that you have raised was the case of Eli Lilly accidentally disclosing information about the takers of Prozac, and I think here is an example of why a private right of action is essential. You could ask: Is the market going to punish Eli Lilly for this breach of privacy? Is it plausible, for example, that a depressive patient sitting in his doctor's office would say, "No, no, don't prescribe me Prozac; I don't like the manufacturer's privacy practices".

No. I think there is a clear failure here of the market to provide a feedback, and if a private right of action were available for $500, then that would clarify the minds of the manufacturers and provide an incentive get its security procedures in place and to ensure that that kind of incident doesn't happen again.

Another example of the private right of action occurred with Amazon. The Federal Trade Commission found in May that Amazon had likely been deceptive in its information practice descriptions that it had given to customers, but it decided to take no action, in part because Amazon had updated its description to conform with those practices.

I think if you take the analogy, as we have heard, with financial information, that if the SEC discovered a company had misled investors in a prospectus but then changed the figures and let them off, we would regard that as unsatisfactory. So I think a private right of action will allow individuals to continue to defend their interests where a Federal Government agency may be disinclined to do so.

The next example I would like to take you raised is safe harbor, which is not an ideal privacy standard in my view, but it is much higher than the average American gets from the average company, and I commend Microsoft for recently announcing that it would adhere to safe harbor, not only for its European customers but also for all customers worldwide.

I have been a long critic of Microsoft because of their failure to live up to their own statements of privacy, but I do hope that they will observe this, and I think it raises the question of whether Microsoft would support such a standard being mandated by Federal law and why these many other companies that have signed on think that the citizens of this country should not have privacy rights equivalent to those which they are willing to grant to other countries.

The next example I would like to raise that you have been discussing is the question of online versus offline. Should higher standards apply to the online world? My answer is yes for collection, but no for other types of issues such as access to information, which I think is very important and onward forwarding of the information. The Internet provides enormous opportunities for the collection of information.

If I go into a physical book shop and look at a title on the shelf, no one is recording that, but an online book shop is. Traditionally Congress has looked at the ability of technologies to invade privacy, and applying one standard to all technology is like saying that a thermal imaging system which can see through the walls of your

house as your body moves from room to room should be subjected to the same privacy standards as a photocopier. This is absurd. It is totally appropriate to have technology-specific controls for collection of information.

But for principles such as the access to the information and for the question of whether the permission of the consumer concerned should be given, provided before it is disclosed for a secondary purpose, then I think the same standards should prevail online and offline.

My third point is about P3P, which I have written extensively on, concluding that it really will not raise the privacy of the average Internet user, and that it has become more a pretext for privacy procrastination than a technology that will improve privacy. But as my time has expired, I will pass to Microsoft to present on that. Thank you.

[The prepared statement of Mr. Catlett follows:]

PREPARED STATEMENT OF JASON CATLETT, PRESIDENT AND CEO, JUNKBUSTERS CORP.

My name is Jason Catlett, and I am President and CEO of Junkbusters Corp., a for-profit company working with businesses, governments and legislators to promote privacy and reduce unwanted solicitations such as junk email. My Ph.D. was in Computer Science, and I have also held various academic positions, most recently as a fellow at the Kennedy School of Government, Harvard University (2001–2002 academic year). I'd like to thank the Committee for inviting me to appear again today, and for its past hearings on privacy.

Rather than repeating matter from my written statement of May 25 last year or from the testimony today of Professors Rotenberg and Schwartz (with which I concur), I would like to examine several events and trends over the past 13 months since I appeared before you all, and ask how they should inform your deliberations. My view is that recent experience reinforces the conclusion that strong comprehensive privacy law is urgently needed, with a private right of action and without the preemption of state law.

Over the past year businesses have admitted that privacy is a problem that is not going to go away without legislation. Executives at companies such as Hewlett-Packard, Dell, Intel, and the American Electronics Association (a large trade group) have called for Federal privacy legislation. Many have advocated a weak "notice and opt out" bill, but several marketing leaders have come out in favor of an opt-in standard. Permission marketing, as they call opt-in, has matured from a radical idea to a mainstream doctrine. Online marketers know that spam (Unsolicited Commercial Email) has poisoned the good will of online consumers, and some trade associations have supported opt-in as the standard for email marketing. As I have testified before your Subcommittee, I believe this standard should be Federally mandated.

The opt-out model has recently been put to a large-scale test, as the weak privacy requirements of the Gramm-Leach-Bliley Act (GLB) came into effect at the beginning of this month. According to a survey by the American Banking Association, 41% of people do not recall having received their notices; clearly they have not been served well by the opt out model. The 36% of people who read their notices may have gained too rosy a picture of the state of their privacy. For example, US Bancorp's Consumer Privacy Pledge opens with the assurance that "Protecting your privacy is important to the U.S. Bancorp family of financial service providers." Four hundred words later, the bank says it allows itself to disclose all of the information it has "to other financial institutions with which we have joint marketing arrangements." Indeed, the bank has not been reluctant make such disclosures in the past. According to Minnesota Attorney General Mike Hatch, it sold to a telemarketing company following information about its customers: "name, address, telephone numbers of the primary and secondary customer, gender, marital status, homeownership status, occupation, checking account number, credit card number, Social Security number, birth date, account open date, average account balance, account frequency information, credit limit, credit insurance status, year to date finance charges, automated transactions authorized, credit card type and brand, number of credit cards, cash advance amount, behavior score, bankruptcy score, date of last payment, amount of last payment, date of last statement, and statement balance." In a pre-

pared statement the bank's CEO characterized this kind of transaction as an "industry-wide practice." Now, I think it is reasonable to presume that if the average American were asked in a plain and direct manner whether she wanted the bank to sell all this information about her to telemarketers, she would say "no". But by failing to find, read, understand, and respond to a privacy notice, she has unwittingly allowed this to happen. Under the opt-out model, banks continue practices against the desires of the majority of their customers, by making their notices ineffective, vague, and bordering on deceptive, and by placing the burden on the consumer to try to understand what they need to opt out of and how. The GLB experience is a clear illustration of the necessity of an opt-in model for disclosure and secondary use of information. In their lobbying against opt-in legislation, banks claimed it would cost them millions if they were required to obtain consent before selling information about their customers. This is an understandable motive, but the question for lawmakers is whose interests should prevail here.

Over the past year the Internet bubble has burst, and some who lobby against privacy for Internet companies have changed their tune from "don't crimp the nascent growth of this new medium" to "don't hit us while we're down." One might wonder whether under this logic there could ever be an appropriate time for privacy rights; I would suggest this time is long overdue. As Professor Rotenberg concluded from a Gallup poll, privacy continues to be a major reason for non-participation, as well as an ongoing concern of online shoppers; this does not decline as users become more experienced. Forrester Research has concluded that "Nearly 90% of online consumers want the right to control how their personal information is used after it is collected. . . . Surprisingly, these concerns change very little as consumers spend more time online." Many online retailers have gone bankrupt or are struggling to achieve profitability, as online consumer spending has failed to grow as quickly as hoped. Unfortunately the many bankruptcies have further damaged privacy, as customer databases of companies that formerly promised never to sell personal information without consent are sold, usually on an opt-out basis. Consumers typically have no option to see the information that is being sold about them, so the opt-out choice is fairly meaningless. This is one reason why access rights should be included in privacy legislation.

At a public workshop run by the Federal Trade Commission in March, the major consumer profiling companies refused to allow people access to their own profiles, or even to provide sample profiles.

Online profiling companies also told the FTC that they are continuing development of their Consumer Profile Exchange technology without any committment to observe fair information practices in their use of it.

In May the Federal Trade Commission found that Amazon and its Alexa division has likely deceived customers, but it decided "not to recommend any enforcement action action at this time," in part because the company had changed its description of its practices. This is a lamentable non-action for a consumer protection agency that is supposed to keep companies honest. Imagine if the SEC found that a company had misled investors with fake figures in a prospectus, then let them off because they had issued new figures and moved into a new business. To me this incident is an illustration of the need for a private right of action. So are many other incidents where companies have made inadvertent disclosures contrary to their undertakings to consumers, most recently Eli Lilly's release of the e-mail addresses of 600 people on Prozac. Companies face too little negative feedback for their errors. What sufferer of depression is going to tell his doctor not to write him a prescription for Prozac because of the manufacturer's record on privacy?

Another trend is that more companies online are posting so-called privacy policies, but the quality of those policies appears to be getting even worse. This conclusion was reached in one longitudinal study by Enonymous. There have also been some prominent examples, such as Amazon.com's change of policy at the end of August 2000. As customer of many years, I was shocked to find after a long and careful examination of their new policy that a company that had previously undertaken never to sell my information, might now sell the title of the next book I bought, in the event of a bankruptcy, or in bulk if they sold a division, such as their book operations.

Dissatisfied, I asked Amazon to delete its records of the books I had purchased. They have repeatedly refused, saying that their systems were not designed to accommodate this easily. They also refused my calls to show their customers all the information they have about them on request. The laws of several countries in which Amazon operates require both access and deletion on request, so I find their refusal to extend these rights to Americans deplorable.

In the past year several nations including Canada and Australia legislated broad, technology-independent privacy rights rights for their citizens, partly with an eye

toward enabling free data flows with the European Union. Some fifty companies have signed up with the Department of Commerce's Safe Harbor program, committing to a privacy standard that in my opinion is short of ideal, but still far higher than most companies provide for their American customers, and higher than almost all proposed Federal privacy legislation. The program applies only to the data of Europeans, but Microsoft has stated that it will apply that standard to all its customers, including the U.S. I wish I could hear an explanation from these companies as to why they don't want their American customers to have mandated by law a level of privacy that they are willing to grant to Europeans.

Ever more intrusive collection technologies are being rolled out, such as online tracking mechanisms, spyware, face recognition systems, location tracking devices and thermal imaging. To the lobbyist who says that the Internet shouldn't be held to a higher standard in privacy law than the offline world, I ask whether he believes that a camera that can see his body through the walls of his home should be held to the same privacy standards as a photocopier. Restrictions on data collection necessarily take into account the means of collection. When it comes to the use and disclosure of information, I generally agree that the same principles should apply regardless of how the information is collected, processed or distributed.

Enthusiasm seems to have waned in the past year for the hope that "technology got us into this mess, so technology can get us out of it." I am certainly in favor of privacy enhancing technologies: my company has for several years published such software, and it has been used by hundreds of thousands of people. But advances in "cloaking" technologies are always outstripped by advances in collection technologies, both in capabilities and degree of adoption. In September American Express announced that it would roll out in 2001 a "private browsing" service with a startup company called Privada. Privada recent ceased operations, and AmEx has told me it does not intend to deliver the service.

P3P has for years been billed as the privacy technology of the future, and it seems destined to remain so for at least several more years. Even if the computer-readable privacy notices of P3P were universally deployed, it would suffer the same problems as human-readable privacy notices that I have listed above. Microsoft has implemented a part of P3P in its next browser, but only as an excuse not to fix the default settings that allows tens of millions of web bugs to gather click streams in volumes of billions of clicks per day. Microsoft's "thermostat setting" where surfers are required to tell their PCs how much they will tolerate being surveilled gives a misleading and dangerous view of privacy. People should not be forced to trade privacy for participation. People need legally guaranteed privacy rights to control the data collected about them.

In July 2000 the FTC sanctioned a deplorably low set of standards proposed by DoubleClick and a few other online advertising companies under the name of the Network Advertising Initiative. Some of these companies are no longer with the NAI, having gone bankrupt or withdrawn on principle to support privacy. The companies require consumers who do not wish to be tracked to get "opt-out" cookies on their browsers. This is bad policy and bad implementation. People generally believe that destroying all their cookies will improve their privacy, and do not realize that this step in fact removes the record of their request to be anonymous. This opt-out feature is a contemptible excuse for massive surveillance.

Mr. Chairman, Members of the Committee, as this collection of a year's events suggests, each week brings another Love Canal of privacy to light. In previous centuries people enjoyed privacy as an accidental byproduct of the practical obscurity of personal information. Those days are gone forever. Privacy will not return to us by accident. Privacy will not survive without strong acts of will by democratic government. Privacy will not survive unless citizens have effective privacy rights created by governments. Privacy requires the diligent efforts of companies and institutions to comply with mandatory standards. Few companies will ask you to impose that discipline on them. But it is up to you to require all organizations that handle information about people to treat it fairly. Unless you do that, our society will not enjoy the benefits that our technology and economy could deliver, and we will be robbed of something that is very necessary to a dignified human existence: privacy.

I appreciate the opportunity to speak before you today. I would be pleased to answer your questions.

The CHAIRMAN. Thank you very much.

Mr. Rubinstein.

STATEMENT OF IRA RUBINSTEIN, ASSOCIATE GENERAL COUNSEL, ELECTRONIC COMMERCE POLICY, MICROSOFT CORPORATION

Mr. RUBINSTEIN. Chairman Hollings, members of this Committee, thank you for the opportunity to testify today. My name is Ira Rubinstein, and I am associate general counsel for electronic commerce at Microsoft. Today I would like to talk to you about our work on Internet Explorer 6, which is the next version of our popular browsing technology and which is available to the public today in a preview version and will be released generally on October 25 when we ship Windows XP.

In particular, what I am going to show you today are tools in Internet Explorer 6 that will make the privacy policies of web sites more transparent to consumers than ever before, and that will give consumers on a broad scale greater control of their online information than they have ever had. These tools will also directly address one of the issues that we hear the most concerns about, online profiling or tracking, which is the practice of collecting the history of a user's actions across a series of web sites.

Before I give an overview of these tools, I want to emphasize that this effort builds on an open industry standard. We have been working with the Worldwide Web Consortium on a technical standard called P3P. The goal of P3P is to provide a common language for a site to describe its data practices, such as what data it collects, how the site uses it, how it handles cookies, and so on. The common language helps web sites describe the important aspects of their information policies according to a standardized road map.

I hope my slide presentation will come up in a moment, but I believe you also have a printout of these slides. P3P also provides a mechanism for a site to provide a machine-readable version of its data policies. The grand vision of P3P is that when sites code their privacy policies according to this standard and consumers have P3P tools in their hands, they can automatically match their individual privacy settings and preferences against the practices of the web sites they are visiting. If the web site satisfies the consumer's preferences, the consumer enters the web site without incident. if the site does not match the individual's personal setting, the consumer at least is warned of that fact before proceeding.

Let me now show you how this will work in Internet Explorer 6, and I would ask you to refer to the handout of the slides until the computer here reboots. On slide 3, you will see a box describing the first-time consumer experience when a consumer connects to a web site whose privacy practices related to cookies and information reuse do not match the consumer settings in Internet Explorer 6.0. When this happens, a small window appears.

By the way, a cookie is a file created by an Internet site to store information on the user's computer, such as preferences when visiting that site or in some cases, personally identifiable information, such as a name or an email address.

The window that appears when a user first connects to a site tells the consumer about a new privacy icon which unfortunately is not on your screen, but it appears in the lower right-hand corner as a small red eye, and it represents a warning that Internet Explorer 6 technology has detected a mismatch between the consumer

settings for accepting or rejecting cookies, and the practices of the web site. I am now on slide 4, which has a large arrow pointing to that red eye icon.

This privacy warning will show up every time there is a mismatch, and this feature by itself does a lot to foster more transparency about privacy policies than has been imaginable in the past. In addition, to offer consumers control, we have provided an easy mechanism that allows the consumer, the individual, to specify how Internet Explorer 6.0 should handle cookies and associated data practices.

I am now on slide 5, which you see has—is labeled, Medium, and has a slighter setting, and the slides are now appearing on the screen. This is the default setting for P3P in Internet Explorer 6, and this setting will ship preinstalled and filter third-party cookies, the cookies that are used to track users across sites. By default, these third-party cookies will be blocked unless the third party provides a machine-readable privacy policy in the P3P format, so that is requirement No. 1, that the site have a P3P policy.

And in addition, on this slide, the user in this case has browsed to an MSNBC site, which is using advertising from MSN and from other sites, but the cookies delivered along with those advertisements did not have the appropriate P3P policies associated with them, so they were blocked, and that is because P3P is still in the early trial stages, and MSNBC, like other web sites, has yet to deploy the P3P compact policies.

So these cookies from a site other than the one the consumer was visiting, the site serving the ads, have been blocked, because these sites have not yet launched their P3P policies. Moreover, even if the third party has a P3P-compliant policy in this medium default mode, its cookies will be blocked if it is reusing a consumer's personally identifiable information and does not allow for consumer choice, either opt-out or opt-in, and this approach tracks the arrangement established last summer between the FTC and the network advertising companies.

With a single click, however, consumers can change the setting to a higher or lower level of privacy. The medium-high setting requires opt-in for third parties' reuse of personal information and at least opt-out if the site you are visiting, a first party site, wants to reuse that personal information. Users can also click to a high setting, which would require all web sites to obtain opt-in consent before the reuse of PI, and you can also block all cookies. There is also a low setting which would allow the user to accept all cookies, which is effectively the current state of the web today.

Internet Explorer 6 has a number of other features that help consumers control their privacy. Most importantly, we have tools that enable consumers to easily capture and read the P3P-compliant policy of a site. While I am not showing all these features today, I would like to mention just a few. We have tools that allow consumers to import settings from some other source besides Microsoft, so that Center for Democracy and Technology, for example, which is an organization that has worked extensively on the P3P standard, is also in discussions with us about developing their own settings which a user could then import onto its browser, and since

P3P is an open standard, other companies could easily develop their own P3P implementation.

Now, we are actively encouraging web sites to deploy P3P policies, and based on feedback so far, we hope to see a very significant deployment. I want to emphasize in closing that we don't view IE6.0 and its P3P implementation as a silver bullet solution to all online privacy issues, but it is a very significant step, and it shows that technology can play a critical role in addressing consumers' privacy concerns.

Fundamentally, we believe we have done work that consumers want and that will retain their trust in the face of concerns over the collection and use of personal information. Thank you, and I look forward to your questions.

[The prepared statement of Mr. Rubinstein follows:]

PREPARED STATEMENT OF IRA RUBINSTEIN, ASSOCIATE GENERAL COUNSEL, ELECTRONIC COMMERCE POLICY, MICROSOFT CORPORATION

Chairman Hollings, Ranking Member McCain, Members of this distinguished committee, thank you for the opportunity to testify before you today on subjects that are very important to consumers—Internet privacy and the tools that consumers can use to protect their privacy. My name is Ira Rubinstein, and I am Associate General Counsel for e-commerce policy at Microsoft Corporation. At Microsoft, we are not only dedicated to protecting consumer privacy, but from an even broader perspective, to building an online community that consumers trust and to promoting vigorous growth of online opportunities for all.

OVERVIEW: THE MARKETPLACE IS DEMANDING BETTER PRIVACY TOOLS

Today I would like to share with you just one of the things our company is doing around the issue of online privacy. For several years, Microsoft has been at the forefront of promoting privacy online. We have been developing privacy best practices and procedures under the leadership of our Director of Corporate Privacy, Richard Purcell. We have been actively involved in coalitions such as getnetwise.org, which focuses on building a safer web for our children. Elsewhere in the company, we are developing futuristic technological tools that have the potential to ultimately transform how online privacy protection is delivered to consumers. Today, I would like to discuss with you the exciting work being done by out Internet Explorer team, the team that is developing the next version of our browsing technology, Internet Explorer 6.0.

Because the web is increasingly important in people's lives, one of the issues customers raise with us more and more is their desire to know that their privacy is being protected when they go online. When we receive such feedback, we attempt to the extent possible to incorporate features that meet this demand and that give consumers better control of their personal information. In the end, it's our job to build software that delights our customers. Because of consumer demand, Microsoft currently has about 25 people working on the privacy protections in Internet Explorer.

INTERNET EXPLORER 6.0: TACKLING ONLINE TRACKING

When we talk to our customers, one of the questions they raise most often is whether their web surfing activities can be tracked. It is an issue that the Microsoft Internet Explorer team has been working to address for about eighteen months now. Tracking or profiling is the practice of collecting a profile or history of a user's actions across a web site or series of sites. When combined with "personally identifiable information," such as name, address, phone number or other identification, whoever collects this profile can market or target advertising or other services specifically to a customer.

Much of the online tracking you hear about comes through the use of "cookies," small benign pieces of information that a web site stores on an individual's computer. It is important to note that cookies in and of themselves are neither good nor bad. Without cookies, the web wouldn't work as people expect it to. There would be no customization, no e-commerce and the economics of the web would be called into question. However, consumers should still be in control of this technology.

Since most online profiling comes through the use of cookies, Microsoft has been concentrating its privacy protection mechanisms in Internet Explorer around cookie management features, which we have designed to enhance notice and choice of the information practices of the web sites that consumers use. Based on our experience with a series of test versions of Internet Explorer and our work with the World Wide Web Consortium's (the "W3C's") Privacy Working Group, we believe that the next version of Internet Explorer—IE 6.0—will take significant strides in protecting consumers' privacy.

One of the most challenging things about building software for tens or even hundreds of millions of people all around the world is that it needs to work in a way that provides the protection consumers want, but without disrupting or slowing their web browsing experience. In some of the earlier test versions of privacy protections in Internet Explorer, we found that consumers were actually frustrated with tools that popped-up questions or prompted the consumer every time a cookie might be used for tracking purposes. It turned out to be too burdensome and confusing for consumers to understand exactly what was going on behind the scenes on their computers.

From the significant usability tests that Microsoft does, we know that if you constantly pop-up privacy questions, users either disregard them or perform whatever action is necessary to make these pop-ups go away. Obviously, this behavior undermines the goal of protecting the user more thoroughly. So we've been working to create a solution that helps consumers to control cookies. And we've been especially focused on so-called third-party cookies that can be used to track your activities across sites—that is, cookies that come from a party other than the site a consumer is visiting. Our tools help consumers better understand the source and purpose of the cookie, thereby giving the consumer more control over whether it is accepted or rejected. Our tools also offer a default level of privacy protection that is greater than exists on the web today, so that out of the box, users of Internet Explorer 6.0 enjoy protections they currently do not have.

PROTECTING PRIVACY THROUGH INDUSTRY STANDARDS

Before we get deeper into the details, let us focus on the role industry standards have played in getting us to where we are today. As our engineers were examining the best path to take to control cookies through Internet Explorer, we were simultaneously working with the World Wide Web Consortium on a technical standard called the "Platform for Privacy Preferences Project" or P3P. The goal of P3P is to provide a common language for a site to describe its data practices—such as what data the site collects, how the site uses it, who gets access to it, how long the data is retained, what consumers should do if they have a privacy complaint, etc. The common language helps web sites describe the important aspects of their information practices according to a standardized road map.

P3P also provides a mechanism for a site to provide a machine-readable version of its data practices. The grand vision of P3P is that once sites code their privacy policies according to the standard, and consumers have P3P tools in their hands, consumers can automatically match their individual privacy preferences against the practices of the web sites they are visiting. If the web site satisfies the consumer's preferences, the consumer enters the web site without incident. If the site does not match the individual's personal setting, the consumer at least is warned of that fact before proceeding.

In Internet Explorer 6.0, we take a significant first step in promoting adoption of the industry's P3P standard by both web sites and consumers. By providing a default level of protection out of the box, we are creating incentives for web sites—and especially those that use cookies in a third-party fashion—to code their privacy policies in the P3P language. These incentives will exist because we anticipate that millions of web surfers will choose to upgrade to IE 6.0 in the near term and will automatically get the protections IE 6.0 offers.

USING P3P IN INTERNET EXPLORER 6.0

Again, based on our earlier research, consumers want to be able to automatically control the use of cookies based on the data practices of the site sending the cookie. The use of P3P technology to help solve this online tracking problem is a natural fit.

How will this work? You can actually test these tools now by downloading the public beta version of IE 6.0 at *www.microsoft.com/windows/ie.* But to go through them quickly, here is an overview. By default, in order for third-party cookies to be set to a consumer's computer, a third party that collects personally identifiable information must indicate, via a P3P-compliant mechanism, that the site offers "no-

tice" and "choice." By notice, we mean that the site provides the consumer a machine-readable privacy policy in P3P format, which clearly states the information collection practices of that party. If there is no notice, third-party cookies from this site are blocked automatically by IE 6.0.

By choice, we mean that if a web site is reusing a consumer's personally identifiable information, then it must allow the consumer to "opt out" of or "opt in" to that data reuse. If personal information is being reused, and consumers don't have choice around that use, then the cookies from that third-party web site are blocked. This approach tracks the arrangement established last summer between the Federal Trade Commission and prominent web advertisers. The core of that arrangement is that a company that tracks users across sites, at a minimum, must provide notice of that practice and the choice of opting out of it.

To help consumers understand the concepts of notice and choice, the first time a consumer connects to a web site whose privacy practices do not match the default setting in Internet Explorer 6.0, an informational dialog-box appears. This box attempts to educate the consumer about a new "red eye" privacy icon that appears at the bottom of the browser window and what this icon means in light of the user's privacy settings. Then, with Internet Explorer 6.0, as users browse other sites that attempt to set cookies but do not meet their privacy settings, the red-eye will reappear, alerting the consumer to potential privacy issues.

While we have taken care to establish what we believe is a workable default setting, we've provided a sliding-scale feature that allows consumers to easily change their privacy settings. With a single click, consumers can change the default setting to higher privacy settings, which have more stringent requirements for the use of privacy policies, or to lower settings, which are less stringent. For example, the "high" setting requires all web sites, both first and third-party, to obtain explicit (opt-in) consent before the reuse of personal information. We additionally have a feature that allows almost infinite customizability of the privacy settings, and we have an "import" function that allows the consumer to download a third party's privacy settings (which, for example, may have default settings different from IE 6.0) and insert them into the browsing technology.

This is just an overview of our technology's features. We are happy to visit with any congressional office to review the tools in greater detail.

OUR OTHER EFFORTS TO PROMOTE P3P ADOPTION

I also want to mention the fact that, in the run-up to the release of IE 6.0, we are actively encouraging web sites to deploy P3P-compliant privacy policies. Through our ongoing work with the top 100 sites on the web, and with the work that the Internet standards body is doing, by the time that Internet Explorer 6.0 launches this fall, we hope to see significant deployment. We've also developed what we call a "Privacy Statement Wizard," an automated privacy statement generator that can help smaller sites become P3P-compliant by creating policies simply based on the site's answers to a series of questions about its practices (subject, of course, to legal review by the site's lawyer). The statement generator is currently available at *http://microsoft.com/privacy/wizard.* It also will soon be available at Microsoft's small business web portal, at *http://privacy.bcentral.com.*

PUTTING IE 6.0 IN PERSPECTIVE

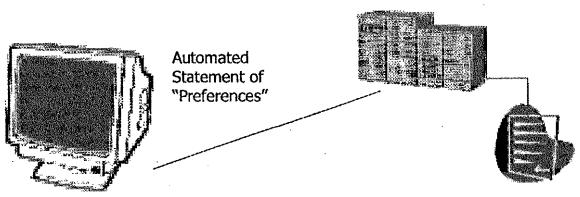
Since P3P is an open standard, not controlled by Microsoft in any way, we believe that other companies will develop additional privacy-enhancing technologies that will also interact in an automated fashion with sites that have posted P3P-compliant privacy policies. In fact, we've already seen the emergence of tools that provide analysis of P3P policies, as well as search engines that only return hits from sites that follow P3P guidelines. Over the long run, we hope to see widespread adoption of P3P by the web community, as well as increasing consumer understanding of the power that P3P tools put in their hands to enhance—and customize—their privacy protection. We believe strongly that P3P is an empowering technology and that it can address in a simpler way the complex questions around consumer preferences and the articulation of sites' privacy policies.

We do not believe that the work we've done in IE 6.0 to enhance consumer privacy is a silver-bullet solution, but we do believe it is a significant positive step—showing that technology can play a critical role in addressing consumers' online privacy concerns. We believe we have done work that consumers want and that will delight them. We also believe that allowing individuals to control their own personal information is an important, enduring mission for Microsoft. It is an ongoing process, and not just a single, all-encompassing step. We take it seriously because our customers do. Finally, we believe that these first steps to include serious privacy pro-

tection in Internet Explorer will lead to positive cooperation in the industry around this topic and will result in a better Internet and a better economy. In the future, we at Microsoft expect to do additional work in this area, using P3P or other technologies, and we would be happy to keep you abreast of those efforts.

Again, thank you for allowing me to be with you today, and all of us at Microsoft look forward to a continuing dialogue.

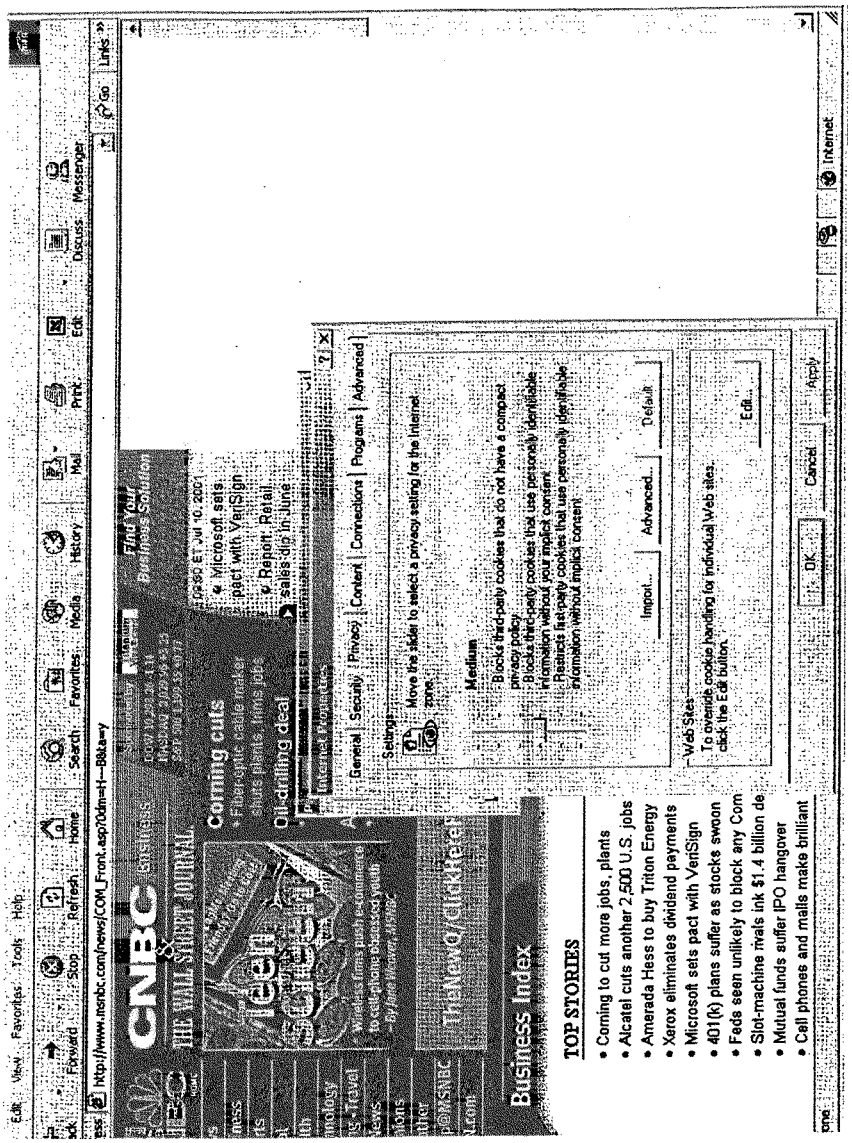
Industry's P3P Standard Can Help Put Users in Control Online



The vision: Before the Web page is displayed, the Web site and user's software determine whether there is a "match" between the site's practices and the user's preferences

CNBC
THE WALL STREET JOURNAL
Business
Find Your Business Solution
Corning cuts
Oil-drilling deal
B/B proposal
TOP STORIES
Coming to cut more jobs, plants
Alcatel cuts another 2,500 U.S. jobs
Amerada Hess to buy Triton Energy
Xerox eliminates dividend payments
Microsoft sets pact with VeriSign
401(k) plans suffer as stocks swoon
Feds seen unlikely to block any Comcast-AT&T deal
Slot-machine rivals ink $1.4 billion deal
Mutual funds suffer IPO hangover
Cell phones and malls make brilliant pair
Business Index

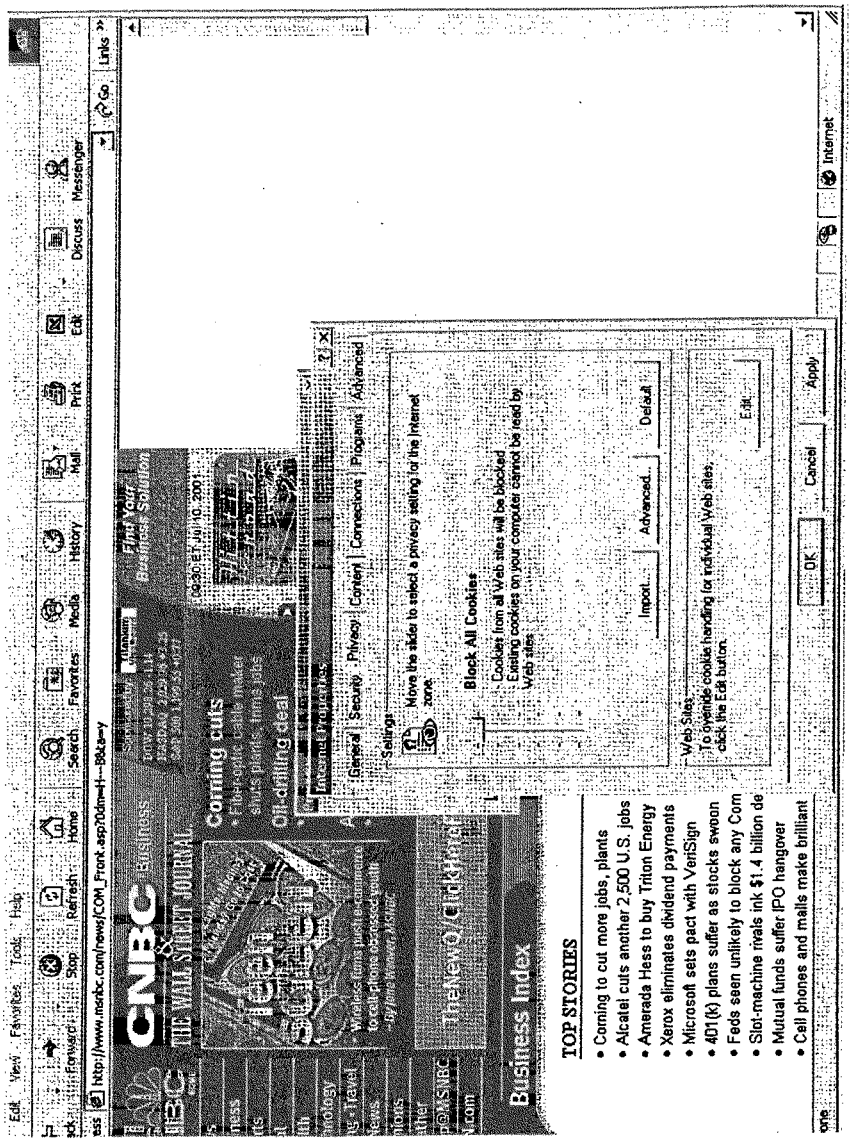
CNBC
THE WALL STREET JOURNAL
Coming cuts
Oil-drilling deal
Business Index
TOP STORIES
• Coming to cut more jobs, plants
• Alcatel cuts another 2,500 U.S. jobs
• Amerada Hess to buy Triton Energy
• Xerox eliminates dividend payments
• Microsoft sets pact with VeriSign
• 401(k) plans suffer as stocks swoon
• Feds seen unlikely to block any Comcast-AT&T deal
• Slot-machine rivals ink $1.4 billion deal
• Mutual funds suffer IPO hangover
• Cell phones and malls make brilliant pair
Internet


CNBC
THE WALL STREET JOURNAL.
Coming cuts
Oil-drilling deal
Business Index
TOP STORIES
• Coming to cut more jobs, plants
• Alcatel cuts another 2,500 U.S. jobs
• Amerada Hess to buy Triton Energy
• Xerox eliminates dividend payments
• Microsoft sets pact with VeriSign
• 401(k) plans suffer as stocks swoon
• Feds seen unlikely to block any Com
• Slot-machine rivals ink $1.4 billion de
• Mutual funds suffer IPO hangover
• Cell phones and malls make brilliant
Internet Properties
General | Security | Privacy | Content | Connections | Programs | Advanced
Settings
Medium
Blocks third-party cookies that do not have a compact privacy policy
Blocks third-party cookies that use personally identifiable information without your implicit consent
Restricts first-party cookies that use personally identifiable information without implicit consent
Import...
Advanced...
Default
Web Sites
To override cookie handling for individual Web sites, click the Edit button.
Edit...
OK
Cancel
Apply
Internet

CNBC
Business
THE WALL STREET JOURNAL.
Coming Attractions
Business Index
TOP STORIES
• Coming to cut more jobs, plants
• Alcatel cuts another 2,500 U.S. jobs
• Amerada Hess to buy Triton Energy
• Xerox eliminates dividend payments
• Microsoft sets pact with VeriSign
• 401(k) plans suffer as stocks swoon
• Feds seen unlikely to block any Comcast-AT&T deal
• Slot-machine rivals ink $1.4 billion deal
• Mutual funds suffer IPO hangover
• Cell phones and malls make brilliant pair

CNBC
THE WALL STREET JOURNAL.
Coming cuts
Oil-drilling deal
Bush proposa
Business Index
TOP STORIES
Coming to cut more jobs, plants
Alcatel cuts another 2,500 U.S. jobs
Amerada Hess to buy Triton Energy
Xerox eliminates dividend payments
Microsoft sets pact with VeriSign
401(k) plans suffer as stocks swoon
Feds seen unlikely to block any Com
Slot-machine rivals ink $1.4 billion de
Mutual funds suffer IPO hangover
Cell phones and malls make brilliant
Internet
OK
Cancel
Apply
Default
Advanced...
Import...
Edit...

CNBC
THE WALL STREET JOURNAL
Corning cuts
Oil-drilling deal
Internet Properties
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Move the slider to select a privacy setting for the Internet zone.
High
Blocks cookies that do not have a compact privacy policy
Blocks cookies that use personally identifiable information without your explicit consent
Import...
Advanced...
Default
Web Sites
To override cookie handling for individual Web sites, click the Edit button.
Edit...
OK
Cancel
Apply
Internet
Business Index
TOP STORIES
• Corning to cut more jobs, plants
• Alcatel cuts another 2,500 U.S. jobs
• Amerada Hess to buy Triton Energy
• Xerox eliminates dividend payments
• Microsoft sets pact with VeriSign
• 401(k) plans suffer as stocks swoon
• Fede seen unlikely to block any Com
• Slot-machine rivals ink $1.4 billion de
• Mutual funds suffer IPO hangover
• Cell phones and malls make brilliant


CNBC
THE WALL STREET JOURNAL
Coming cuts
Oil-drilling deal
Business Index
TOP STORIES
• Coming to cut more jobs, plants
• Alcatel cuts another 2,500 U.S. jobs
• Amerada Hess to buy Triton Energy
• Xerox eliminates dividend payments
• Microsoft sets pact with VeriSign
• 401(k) plans suffer as stocks swoon
• Feds seen unlikely to block any Com
• Slot-machine rivals ink $1.4 billion de
• Mutual funds suffer IPO hangover
• Cell phones and malls make brilliant
Internet Properties
General
Security
Privacy
Content
Connections
Programs
Advanced
Settings
Move the slider to select a privacy setting for the Internet zone.
Block All Cookies
Cookies from all Web sites will be blocked
Existing cookies on your computer cannot be read by Web sites
Import...
Advanced...
Default
Web Sites
To override cookie handling for individual Web sites, click the Edit button.
Edit...
OK
Cancel
Apply
Internet

CNBC
THE WALL STREET JOURNAL
Coming cuts
Oil-drilling deal
Read the latest Business & Money
TOP STORIES
• Coming to cut more jobs, plants
• Alcatel cuts another 2,500 U.S. jobs
• Amerada Hess to buy Triton Energy
• Xerox eliminates dividend payments
• Microsoft sets pact with VeriSign
• 401(k) plans suffer as stocks swoon
• Feds seen unlikely to block any Com
• Slot-machine rivals ink $1.4 billion de
• Mutual funds suffer IPO hangover
• Cell phones and malls make brilliant
Business Index

The CHAIRMAN. Very, very good.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. Mr. Chairman, I think it has been excellent hearing. It has really been a 3-hour teach-in on privacy and what it is going to take to get this done.

Gentlemen—and let me start perhaps with the Earthlink, Amazon, and Microsoft witnesses. The reason I asked about Eli Lilly really 3 hours ago is that I am concerned that we are headed for an *Exxon Valdez* of privacy. That was a very serious problem with Eli Lilly, but I think with the bad actors that all of you have told me exist out there in the private sector, that we are headed for something far, far worse. If that tragedy takes place, you will not like the legislative response that comes from the U.S. Senate, just as sure as the night follows the day.

So my question to you is: Given the fact that you have really one chance for one standard, one chance to get a preemption bill, what would you all at Earthlink, Amazon, and Microsoft want in terms of your efforts to try to work with us to see if we can get you something that is reasonable? Let's start with the Earthlink folks, then Mr. Misener, and then Microsoft.

Mr. SEAGRAVES. Senator, what we are looking for is something that gives our customers the information they need to make informed choices. The components of that would be something that is simple, something that allows technology to step in, and something—or legislation that actually does something, that gives them and promotes good information given to customers.

Senator WYDEN. So, in effect, what you have just said is if the bill has the elements of the Federal Trade Commission legislation and they would be binding and enforceable, that would be something you would support if you could get preemption in return.

Mr. SEAGRAVES. I think you could basically codify the FTC guidelines, have the FTC enforce them. We could live with that.

Senator WYDEN. Good. Amazon?

Mr. MISENER. Senator Wyden, that is an excellent admonition to us in industry as a matter of sort of legislative strategy. We already comply fully with the requirements of your bill. OK. Amazon.com is already doing this pro-privacy, notice, choice, access, and security on our own in response to our customers' demands and desires, and so we are very proud of that, and we certainly could live under the requirements of the bill that you and Senator Burns introduced in the 106th Congress.

All I have said and all Amazon.com has indicated is that there is no inherent need for legislation, because we believe the market is already driving companies like Amazon——

Senator WYDEN. But how do you deal with the bad actors? See, that is the point. The fact is there are a lot of people out here who don't work closely with Chairman Hollings and Senator McCain and come to hearings that examine this, and those are the kind of people that I think are most likely to produce that Exxon Valdez and do a great deal of damage to the good work that you all have done. You all have worked too hard at building up the credibility of this industry to lose it for some bad actors, and that is why you need a piece of legislation.

Mr. MISENER. Senator Wyden, you make some very compelling points, and I have to say that the points are so compelling that we will continue to examine them going forward. I will say, though, that the incident with Eli Whitney is unlikely to be prevented by the sorts of legislation we are talking today. It was an inadvertent mistake. It is not forgivable in many senses, but the legislation alone won't bar it.

Second, the bad actors——

Senator WYDEN. Just so you know and the record is clear, no bill is ever going to bar accidents. The reason I asked the question—and I think the answer was good—is we would like to reduce the risk, and I am convinced that well-written privacy legislation can reduce it. I interrupted you.

Mr. MISENER. That is quite all right. I just want to conclude by saying that the bad actors that are out there are going to lose in the marketplace. We have well over 30 million customers who have said that we have good privacy policies. They have come to us, and they feel comfortable with us. They trust us. We believe those bad actors will lose out. The little ones that are out there, I think it would be very difficult to enforce against in the first place. There it is, Senator.

Senator WYDEN. But once the bad actors have damaged the credibility of your work and harmed a lot of people, it is going to be too late to put the horses back in the barn.

Mr. MISENER. I fully agree, Senator, and there happens to be a history in Washington of companies who have done good things, to come to Washington and ask for legislation that essentially mimics them so that we erect—so that Government erects high barriers to entry, so the competitors can't come in and compete with those companies like Amazon.com who have done the right thing. We simply have tried to be more pure than that and not ask for that kind of preemptive legislation.

Senator WYDEN. We are going to go at this in a way—and you have heard it from both sides of the aisle—that is not going to freeze technology, and we have worked with you enough to know that I feel very strongly about that.

Microsoft?

Mr. RUBINSTEIN. Senator Wyden, if I might just briefly follow up on two comments that Mr. Misener made and then directly answer your question about legislation, first on the question of accidents, I agree with both of you, that legislation itself is not in a position to prevent accidents and the Lilly situation seems to have been a mistake rather than some intentional act.

Second, on the question of bad actors, I think there is no such thing as 100 percent compliance. We haven't heard much about self-regulatory efforts in this hearing, but let me just mention one point which is that the reach of organizations like Trust-E and other CL organizations is growing and is significant. Let me give you a few statistics. Trust-E is now at 2,000 licensees, which is about 50 percent growth over last year. Seven of the ten top web sites by traffic are Trust-E licensees; 50 of the top 100 sites are licensees. And these licensed sites reach about 145 million web users. So the reach of the self-regulatory organizations is not small today.

On the question of legislation directly, like—Amazon described a bill that is representative of the principles that a number of major industry trade associations have articulated for acceptable legislation, and Microsoft does not oppose legislation per se, and we have been in many of your offices to, you know, review and comment on bills that have been introduced.

But like many in industry, we believe that Congress needs to move very deliberately and very cautiously on this question, both because it is complex and in order to avoid either harming the Internet industry, which is still in its early stages despite some of the comments about legislation being introduced early. Yes. The Telephone Act was introduced in 1936 with privacy legislation, but the telephone was introduced in the 1890's.

Senator WYDEN. Can I just ask one other quick question?

The CHAIRMAN. Surely.

Senator WYDEN. Thank you, Mr. Chairman.

Just one question about P3P, if I could, Mr. Rubinstein. What is it going to take on the enforcement side to make P3P work, because it is very clear that this is useful product. I share Senator Kerry's view in that regard, and it is going to be particularly helpful because it is going to help consumers determine what a web site says it is going to do, but then if web sites say one thing and then do another, we have got an enforcement issue, and Senator Hollings has given me this extra time.

Could you just tell us how envision this enforcement scenario going forward?

Mr. RUBINSTEIN. Yes. I think that is a very good question, and you are alluding to the fact that P3P by itself provides no information about a site's practices but only its policies, and I think that is true of any technological means for understanding what a site does. There is no way of measuring practices through the interactive medium of the web.

What I think that P3P may be able to provide going forward, however, is additional information, for example, about whether a site is a subscriber of Trust-E, has been audited by one of the Big Five accounting firms that does that kind of auditing, and users may well want to set their P3P preferences so that they only do business with sites that so indicate, and I think it can provide greater transparency about enforcement, but there is no way that it could ultimately be a mechanism to demonstrate, you know, practices at the moment.

Senator WYDEN. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you very much.

Senator Allen.

Senator ALLEN. Thank you, Mr. Chairman. First, I want to comment you, Mr. Chairman, for an outstanding and very balanced panel, two panels of witnesses. This is an issue of great interest to me and on the Republican side, chairing the high-tech task force, some of these folks we heard, and trying to find some balance and logic if government action is going to go forward—and I think there will probably be some, but let's make sure it is the most beneficial and not anything to thwart the advantages to our life and our education and information afforded by the Internet.

I would like to follow up on Senator Wyden's comments. He asked many of the questions I would, as well as what Senator Kerry mentioned. I very much agree with the thoughts and processes through there, and in listening to the various witnesses here, and I do think it is very important as we go forward that we do make that distinction between the different types of information, whether that is medical information, health-related information versus financial versus regular consumer information.

And I do think we need to look at each of those categories differently for the levels of protection that people should get from the Government versus the other view of the libertarian view which is generally mine of *caveat emptor* and making sure people are informed, knowledgeable, and they make those decisions and are responsible for the consequences. When you get to health information or privacy in financial, that is a different situation. We do need to have protection, stronger protection there.

Now, Mr. Catlett mentioned that since the Internet, this mode of information or communication is different than the mail or the telephone, but you still use the same principles in applying those basic principles to however the regulations would be. And, indeed, the privacy bills that have been introduced over the years, the way I have looked at them, deal with only information collected via the Internet. But if you look back in history—and I mentioned this a few weeks ago.

I had lunch with some folks from UPS, and when they started off, one of the key things for them getting business was to make sure when shipping packages from Macy's, they wouldn't let Gimbel's know what they were shipping, and Gimbel's wouldn't know what—vice versa, Macy's and Gimbel's.

And so when you hear Mr. Seagraves talk about Earthlink and what you are doing in trying to get a market niche that way and getting more consumers or customers because of what you do, that is responding to market forces; the same way with Amazon.com. Microsoft's involvement in all this is trying to come up with something that they hope consumers will want. And so here you have an example of various enterprises that are responding to the desires. You just have these polls, people concerned about privacy and misuse of information, abuse of information.

These three enterprises are all trying to respond to consumer demand, and I want to commend you all for that, and you will be a model, I think, for us, and it was very interesting. I was taking notes as to the different views that you would have as far as notice and choice, preemption, online, offline distinctions, but you generally don't think there should be distinctions, and as far as legal aspects of it, so I think that what we need to do is listen to the creative technologists and listen also obviously to those in the private sector and make sure that we don't do something that thwarts your industry.

However, the technology or e-commerce industry is going to need to come up with these ideas for you to grow. Otherwise, I think it will thwart the growth of e-commerce and the use of the Internet if people are fearful that their information, their personal data, will be misused or be subject to spamming and other aggravations in

people's lives. There are things that are more than an aggravation, but an infringement that we don't think is appropriate for it.

So I would only conclude by asking this question, following up on what Senator Wyden asked of Mr. Rubinstein, and that is: In the event under P3P that someone—you were talking about, Here is their policies; their question is their practices. And, again, commending all of the entrepreneurs here and their companies, but in the event that their practices don't comply with their policies, what laws currently apply? Would consumer fraud? Would fraud? It is clearly a violation—I would think some sort of a violation, a misrepresentation. What current laws would apply to a company that as a practice knowingly violates the policies that they set forth to the public as far as privacy is concerned?

Mr. RUBINSTEIN. Senator, the situation you described seems to clearly invoke the FTC's jurisdiction under Section 5 of the FTC Act. P3P presupposes that a site is presenting its policies in a written statement, and if it misrepresents its practices based on that policy or it deceives its customers, then it is clearly subject to FTC enforcement action.

I think further, going back to my point about P3P also being used to identify which sites are enrolled with Trust-E or other self-regulatory organizations, if such a site was subject to an FTC action and found to have engaged in illegal conduct, it would have to lose its Trust-E or BBB Online seal, and that would have to also be reflected in its privacy statement, so that P3P tool would eventually detect that.

Senator ALLEN. Thank you. That answer fits into what Senator Kerry—one of the various points you were making Senator Kerry is that in this legislation, I think it would be advisable to make sure that we put in the legislation, at least cross-references if not the complete replication, of all the existing laws that do apply, a variety of areas. You were talking about in your past experiences, the mistake not making sure that you listed a lot of different statutes which already do apply, but I think it is important for folks to understand that they are not without recourse with some of these ideas currently. But I think maybe those can be embellished or reinforced in such legislation.

My time is up, but, Mr. Chairman, again thank you for this very balanced and informative discussion here for our Committee. Thank you.

The CHAIRMAN. Thank you very much.

Senator Kerry.

Senator KERRY. Thank you, Mr. Chairman.

I thank the witnesses for their comments. Let me mention that our legislation will have some pretty strict fines and penalties under the FTC jurisdiction, and there is a clear FTC enforcement mechanism that may need to be strengthened.

Mr. Rubinstein, if I could just ask you. Looking at your handouts here for a moment, if I were to have come in under your new—under the 6.0 that is coming out, if I went to this web site for CNBC, *Wall Street Journal,* will there be an automatic pop-up of this window as I see it, or do I have to go down and hit the icon down here in the bar?

Mr. RUBINSTEIN. That is a very good question. The way we have designed IE6.0 is that this window pops up the first time a user visits a site where its privacy settings don't match the site's policies, but it does not pop up every time. When we first began experimenting with cookie management and with P3P in an earlier version of the browser, Internet Explorer 5.5, we used that type of approach, and even myself, experimenting with that beta version, the first time I connected to a site that I go to almost daily, I got 40 pop-up screens, and like any other user, I quickly turned the feature off.

So we were particularly concerned about not bombarding users with repetitive warnings or notices that would either distract them or lead to a disinterest and thereby really undermine this whole chicken and egg issue of how you get—they are deployed.

Senator KERRY. But the first time I were to go to any particular web site, whether it is informational or transactional, you are saying that the window itself would pop up.

Mr. RUBINSTEIN. Well, let me be very clear about this. This window pops up—we call it a first-time user experience. It is not going to pop up at every new web site you visit. It is going to pop up the first time you visit a web site where there is a mismatch between your setting, which is going to be the preinstalled——

Senator KERRY. Right. That is under the P3P.

Mr. RUBINSTEIN [continuing]. Default setting. And what this tries to do is then immediately educate you at this point when you first see it as to, you know, what this icon means, what cookies are, what the medium default setting represents. If you are then satisfied with that setting, this screen won't pop up again, but if there is a mismatch at some other web sites, the red eye icon will pop up.

Senator KERRY. Fair enough. So the first time, in effect, the first time you are user, then, of your new program——

Mr. RUBINSTEIN. Yes.

Senator KERRY [continuing]. Effectively and you go to a site, you are going to be given the opportunity on that first use to click in the settings you want, and among those settings is the opportunity, I notice, to block all cookies.

Mr. RUBINSTEIN. Yes. And there are also—there is a button for advanced settings which allows some other interesting capabilities, namely you can block or accept all cookies from a particular web site, so if you distrust a particular web site, you add that to your list of blocked sites, and if you like a particular web site, you can say, "Don't ask me again about that site, because I am comfortable with them".

Senator KERRY. In effect, you are really giving—and I am not advertising for you, but it seems to me a fairly complete, broad set of choice. I mean, if we are looking at the choice application here, this is pretty broad consumer choice. You can actually set in—I mean, this is opt-in and opt-out simultaneously.

Mr. RUBINSTEIN. I guess it is opt-in with respect to the settings. I don't want to oversell it.

Senator KERRY. Well, I am not trying to—I don't want to overcharacterize it either, but I am trying to understand it properly . I mean, it seems to me that if I can—if I——

Mr. RUBINSTEIN. I would have to say, Senator—I am sorry to interrupt, but I would have to say that it is opt-out, because it shifts with the default setting, and unless the user changes that——

Senator KERRY. I see. Unless you change the setting, you are automatically stuck with the cookies.

Mr. RUBINSTEIN. Well, you are automatically stuck with the—if you will, with the medium setting, and the medium setting, as I said in my oral remarks, has two requirements. One is that the site has a P3P policy regarding cookies, and the second is that it offers choice in the form of either opt-in or opt-out for third-party cookies.

Senator KERRY. Fair enough. Now, that is—what does this say to us about the P3P? I mean, if you don't have P3P out there, this isn't going to work.

Mr. RUBINSTEIN. If—well, that is correct. If a site doesn't have a P3P policy, this doesn't work in the sense that the full level of information that might otherwise be available, as well as all of the features that might be available, aren't there, but if a site doesn't have a compact—a P3P policy, the red eye will appear.

Senator KERRY. Immediately.

Mr. RUBINSTEIN. So what we are hoping to do is to incentivize sites to deploy P3P policies in order to avoid having that red eye appear, and we have also developed tools, as have other companies like AT&T, called privacy statement generators, and these are automated ways of generating a P3P policy. They are very easy to use. You fill in a questionnaire online, and it spits out a policy which a site ought to have its own privacy officer or in-house counsel review, but it makes deploying these compact policies very straightforward and very easy.

Senator KERRY. Now, Mr. Misener and Mr. Seagraves, let me ask you a question. There is sort of increasing discussion among various companies and players within the Internet world, and you certainly see it behind the scenes, and you see it in some of the trade discussion, that opt-in may not be as critical as some people originally thought, opt-in versus opt-out, and that, indeed, perhaps even the sort of advertising fears that people had are now not as germane, simply because some people are questioning whether or not that model is working at all.

Would you like to comment on both of those observations; the notion that there seems to be maybe an increasing acceptance within the industry that this is not as key as some people though it was originally? And also would you comment on whether or not advertising appears to be as much a concern as people had, because maybe the marketplace has made that decision or is giving strong indicators about it at this point in time.

Mr. MISENER. Senator Kerry, thank you. In Amazon.com's view, the important thing is always to provide our customers meaningful choice, and without trying to characterize it in all instances as either opt-in or opt-out, it should always be meaningful. I mentioned before in my testimony that Amazon.com, in its effort to provide our customers that kind of meaningful choice, often provides what we would call opt-in choice, in other instances provides what we would call opt-out choice. The importance is it is meaningful.

For example, when you go to our ToysRUs.com co-branded site, which provides some toys for some of our customers, you go there,

and Geoffrey the Giraffe from ToysRUs is sitting—there is a little picture of him sitting inside an Amazon.com box. It is very clear in just that little picture what is going on here. There is a ToysRUs.com product being delivered by Amazon.com.

And there is a whole bunch of wording around it as well that explains what exactly is going on there, but that is far more meaningful for the vast majority of consumers out there than having to read some words about policy. We have told them in this little picture instantly: this is a ToysRUs product being delivered by Amazon.com. We thought that was much more useful and meaningful for them than simply providing the words, which we also provide.

Senator KERRY. Right. But coming back to this whole question that Mr. Brondmo raised very clearly and, I think, logically as he went through the progression, sort of, who owns this asset. What is the asset, who owns it, and what use is it put to, is really the issue. And you are sort of going around that in a sense. You are saying, "Well, we give this information to them, but that doesn't deal with the secondary marketplace issues of the information".

And so I am trying to get at, you know, how critical—I mean, the fight here was ostensibly whether opt-in was going to lose people, a flow of information that was going to be important to them in terms of their revenue stream, and ultimate control of an asset. And that is what we are arguing about.

And my question to you is: Has that changed a bit now? Has this marketplace in the wake of sort of the shake out and some maturity and evolution, has it changed in a way? I mean, Mr. Seagraves was talking about the upside benefits of marketing the fuller measure of privacy, and I am wondering if you think it has changed. Is there some legitimacy to this current discussion?

Mr. MISENER. Oh, absolutely, Senator. I appreciate the question. Amazon.com, in its initial privacy policy notice, had indicated that it might at some point in the future sell consumer information to third parties such as telemarketers. Well, we never did that, and we concluded last year that we never would do that, because our customers wouldn't like that, and so we said in our updated and enhanced privacy policy last year—we made a pledge that Amazon.com is not, emphatically not, in the business of selling customer information. We want to protect that customer information, because our customers think it is important.

And you are right. There was this shift where, earlier on, we thought we might do that, but we concluded last year that no way would we do that.

Senator KERRY. Mr. Seagraves.

Mr. SEAGRAVES. Well, as I said, Earthlink does not, you know, really fall one way or the other right now, because we don't—we are not asking the customers, because we don't sell their information. However, that could change so we would need to make a choice. Do we want opt-in or opt-out? And I think there is a tradeoff.

Senator KERRY. Do you think it makes a difference?

Mr. SEAGRAVES. I think it does make a difference, and the tradeoff is this. If you are opt-in, then these are customers that actively say, "Yes, we want you to do this". Then that information is more valuable, although you have much less of it. If it is opt-out, you

have a lot more people that, you know, participate and that will give—allow you to use their information. However, it is not as valuable, because basically they may have just been lazy.

So, you know, I think you need to balance that as far as the particular business that you are in. In our case, I think the value of the information is mostly in bulk, and the targeted information that you get with opt-in isn't necessarily all that important to us.

Senator KERRY. Fair enough. Mr. Brondmo, do you want to comment on that at all?

Mr. BRONDMO. Senator, I think you are keying on something very important here, because there is obviously a maturity that is happening in the marketplace, and we are learning, and that learning has to be brought into any future legislation.

My learning in this area has been—I can maybe illustrate that with a brief example. I worked with a large music retailer a few years ago, and the music retailer was very hesitant to take people off their lists as they were marketing to people, and we were strongly encouraging them to do so, due to an increasing customer satisfaction problem they were experiencing. Their rationale was very reasonable. It costs us a lot of money to get these people to come to our site, to get them into our data base; why should we be making it easy for them to get off our site or to not participate?

Finally they did a test. They learned that it had no substantial impact on their business, because the people that didn't like hearing from them didn't mind, but more importantly when they made it very clear up front on their web site how easy it would be to get off their systems, what they actually found was an increase in subscription. They found more people coming in and opting in or not opting out of the program up front, because they knew it would be simple and easy later on.

Senator KERRY. Now, if there were a prohibition on any unconsented transfer of financial information, i.e., credit card or personal identifier, Social Security number, and so that all that you had conceivably as this asset was a particular purchase, item of purchase, series of items of purchase, location of purchase, date, time, et cetera, and that was the asset, in effect, is there any harm in that transfer, if it were in an opt-out? And is there, in fact, conceivably a countervailing benefit to a consumer that hasn't even been weighed in this discussion? Do you follow me?

Mr. BRONDMO. I am not sure I do.

Senator KERRY. Well, for instance, if the asset that a company has that it either transfers to one of its subsidiaries or sells to another company is information about someone's purchase, but it is effectively an almost anonymous piece of information—not completely; has their address, has a place, knows what they purchased, and therefore, that company wanted to know that, because they want to make a secondary solicitation of some kind, is there some kind of harm done in that, absent any transfer of any personal or financial information, no credit card numbers, no Social Security number, no—nothing but the transaction itself, in effect, which is supposedly the value people want to hold onto for marketing purposes.

My question is: Is there any harm whatsoever to that consumer that is different from the harm in the offline marketplace today,

and is there conceivably an upside benefit to them that hasn't even been weighed in this discussion?

Mr. BRONDMO. Senator, I believe there is potential harm that can be brought to the consumer in the scenario you outlined. The primary problem is that if I visit Amazon, I might look at a number of books. I might leave behind a trail of information which I have no problem trusting to Amazon, but if I knew that Amazon would turn that around and—let's for a moment say that I had political ambitions, and Amazon would sell that information to anybody who would pay $1 to buy it, and all of a sudden somebody could come in and look at what books I had bought, what research I might have done, maybe books that didn't necessary reflect my opinions or my position, but that information being available, I believe that that could potentially be very sensitive information.

I also believe, by the way, that Amazon would be undermining their own business by giving that information away, because that is an insight into my relationship that I have developed with them, which is a key competitive advantage that they have over their competitor, and they should not be selling that information.

Senator KERRY. But that information is available today in the offline world and even worse is available today. I mean, look at what happened to Justice Thomas in his confirmation process. We learned what Monica Lewinsky's videos were, I do believe. I mean, we have had, you know—offline world, you can do that today.

The CHAIRMAN. You don't think we can regulate it, do you?

Senator KERRY. That's my question.

Mr. BRONDMO. Well, Senator, that does not change my opinion with respect to the online behavior.

Mr. MISENER. Senator Kerry, you are absolutely right. Just to answer, of course, Amazon.com does not do what was discussed just a moment ago. It does make little sense, however, to enact a law or put in place a regulation that would only govern one medium.

Senator KERRY. Well, I agree. This is the point that I have been making for some period of time on this Committee, that if the right of privacy is what we are talking about, it seems to me that if you are providing adequate protection for the flow of financial information, et cetera, if it is the marketing concept, that is available in any number of ways, through credit bureaus. I mean, the information that appears on people publicly in America today is stunning.

And there, you know, it seems to me we have got to look at this considerably differently or more broadly, I suppose, is the way to phrase it. But, I mean, would Amazon—would somebody be able to find out—Senator Rockefeller was asking me that in a private conversation. I mean, if, for instance, somebody went in and had a whole series of books that they got because there was a particular family crisis going on or someone was sick with a particular disease and they start—all of a sudden they have ten books on a particular subject, would those books then be traceable, and therefore, they will be suddenly solicited by therapists or psychiatrists or a whole bunch of people because they seem to have an inkling that that is an area those folks are now concerned about?

Mr. MISENER. Absolutely, emphatically not. Amazon.com will not share that sort of information at all. We will share in certain circumstances information resulting—or applying to a particular

transaction, e.g., a purchase of wireless services through our wireless services store, but only in an opt-in circumstance. The wireless store does not get, for example, information about the pots and pans that I may have purchased or the books that I may have purchased, only resulting from that, but again that is an opt-in circumstance.

Senator Kerry, you are right on point, because 99 percent of the retail transactions in this country last year were done offline, so to the extent we apply a new law only to the online world, we are only touching a very tiny percent, and those transactions are only those made by those fortunate enough to be on the fortunate side of the digital divide. Those who aren't get none of the benefits.

Senator KERRY. And what do you say to people who distinguish the online world because of its interconnectedness and capacity to conglomerate transactions which doesn't occur when you walk individually into a particular store?

Mr. MISENER. It is a good question. The capacity to conglomerate is not inherent only to the online world. The data bases exist no matter where you are. In the offline world or wherever, those data bases, that information about you, generally far more sensitive information than Amazon.com would ever collect, exists in the offline world. To the extent there are differences—and I think there are some, but they are very limited—to the extent there are differences, for example, third parties tracking you around a site, legislation at that point would be something that could be appropriate. Amazon.com bars that.

We do not allow third-party cookies to be served on our site for that very reason. We don't think our customers should be subjected to that sort of thing. That is different from the offline world. But where there are similarities, information collected, information used for marketing purposes, then it ought to be treated the same.

Senator KERRY. Well, I thank you very much. It is obviously a very important area. I just want to emphasize again, for the benefit of where we are heading here with the Chairman that I think he is right on target in terms of where we need to be and being very declarative on the medical and the financial and so forth. And I think we need to sort of sort through the other components of this that we have discussed today.

Mr. Chairman, this has been a good hearing, and I thank you very, very much for your leadership.

The CHAIRMAN. I thank you very much, Senator. It has been an outstanding hearing. I have learned a lot, and it strikes me that—and you can always get in trouble thinking out loud, but there is no question that we have got to legislate, but we have got to legislate cautiously. So in the sense that we legislate cautiously, some would legislate, as others have introduced bills last year with opt-out alone, or the FTC guidelines which are optional, and neither approach has worked. We tried that with the banking bill, and that's a big uproar as the witnesses testified, that it is not working.

So you look at the best of the best, namely Microsoft that opts in for our opt-in, and Schwab, the best of the best analysts, business-wise says it's not really that much of a burden; in fact, it is a good business practice. And you find just that. The best of the best thinks they make money out of privacy, namely P3P, and oth-

erwise, you have already joined in to the European safe harbor, and as an American politician, I am saying to myself, "Well, can't I give the American citizenry an equal protection as those citizens in Europe", unless there is something wrong with that safe harbor.

Is there anything wrong with that safe harbor that you know about, Mr. Rubinstein, that you want the Committee to know about?

Mr. RUBINSTEIN. Well, I do want to comment on the safe harbor. Microsoft and some hundred other multinationals have signed up to the safe harbor, but I think we should be very clear about what the motivation is.

The CHAIRMAN. Well, I know the motivation. You all want to do business in Europe. Go ahead.

Mr. RUBINSTEIN. Well, that is exactly correct.

The CHAIRMAN. Sure.

Mr. RUBINSTEIN. As a multinational, we are bound to comply with European law.

The CHAIRMAN. Whoopee. That's right. We are in a global economy. Every time you mention something around here, some politician jumps up and says, "Well, this is a global economy. OK. So we can pass that point".

Mr. RUBINSTEIN. But if I can offer an analogy, France has laws regarding the use of French language on web sites operated in France. The fact that Microsoft complies with those laws does not in any way apply that we advocate English-only web site laws in the United States, so I don't see——

The CHAIRMAN. But you have, on the opt-in, you have opted in. Microsoft favors opt-in.

Mr. RUBINSTEIN. We favor opt-in in an evolving business model, namely what we call our Hailstorm Services that are premised entirely on two things. One is identity management, so those services are all about the most sensitive and personal information, and No. 2—and I think this is the theme that has been reflected in all of the comments today—those are subscription-based, fee-paying services. They are not free web content or free services, and in that context, we do not favor opt-in legislation at all.

The CHAIRMAN. Well, that is the fundamental question. What is sensitive? Medical, personal medical and personal financial. Right?

Senator KERRY. Chairman, can I mention——

The CHAIRMAN. Yes.

Senator KERRY. Chairman, I just wanted to say that I approached this with—I was on the conference Committee, on the Banking Committee on the Gramm-Leach-Bliley, and I voted then and we lost on the more stringent opt-in requirements, and we have seen the results of that. So I think there are some lessons we can draw from both the maturity of the industry, but also from what has happened in terms of the regulatory application process.

So I hope, Mr. Chairman, we can—I think there is room—I thought there was a lot of sense of possibilities and wisdom from both panels about the capacity to sort of combine the pieces here and try to draw some distinctions between the areas of sensitivity and the commercial side, and maybe we can do that.

The CHAIRMAN. Oh, yes. We are going to do it very cautiously, but I hope we can get something done. What happens is that we

have got to look into that matter of preemption and perhaps with the states, let them operate upwards on that score. And otherwise there will be a debate and probably a difference of opinion with respect to the private right of action that Mr. Misener absolutely opposes.

Mr. Misener, what we have found from hard experience—we had a hearing just last year with respect to the Firestone tires, and the National Highway Safety Transportation Administration, NHSTA, and we asked the Secretary—we had 99 million recalls in the past 3 years. This was last year's hearing, and we asked the Secretary of Transportation how many had been required by NHSTA. Zero, none, in the 99 million recalls. They were all done on account of the Pinto case.

And everybody knows that—in fact, we only found out about the bad tires from personal causes of action and some 200 deaths. That is how it came to our—I never had heard about it happening in South Carolina or anywhere else until we found out people were dying in Saudi Arabia, dying down in Venezuela, and they had been given notice and everything else like that, and now we find out we had 200 in this country.

So that is why we even consider a personal cause of action. Somebody thinks, well, this is all lawyers and trying to get lawyers cases and everything else of that kind. What we are trying to do is go in in a deliberate fashion, and as Mr. Seagraves says, not produce a regulatory mine field and not overreact. Nobody is vindictive about it. And you folks have been unusually helpful to this Committee. We will probably have perhaps another hearing, but we are going to work it out.

And we will leave the record open for any further questions by either the members that could not attend, and otherwise for any comments and further information you would wish to finish the Committee. The hour is late. The lunch is ready. Thank you all very, very much.

The Committee will be in recess until the call of the Chair.

[Whereupon, at 1 p.m., the hearing was adjourned.]